1.0 Section 5: Vendor Proposal

Per RFP Section 5.3, Proposal Format instructions, First Data Government Solutions, LP (FDGS) provides our technical proposal on the following pages. The Technical proposal does not contain any cost information relating to the project. The Technical proposal is structured as outlined in ***Table 11: Expected Proposal Sections and Content Structure*** of the RFP.

RECEIVED
2020 MAR 11 AM 9:31
WV PURCHASING
DIVISION

1.1 Title Page

Technical Proposal	
RFP Subject:	West Virginia Department of Health and Human Resources (DHHR) for an Electronic Visit Verification (EVV) Solution
RFP Number:	CRFP 0511 BMS2000000001
Vendor Name:	First Data Government Solutions, LP
Business Address:	5565 Glenridge Connector NE Atlanta, GA, 30342
Telephone Number:	(513) 878-8123
Fax Number:	(402) 315-5105
Contact Person:	Mr. Grant McKay 11311 Cornell Park Drive, Suite 300 Cincinnati, OH 45242
Email:	grant.mckay@fiserv.com
Vendor Signature:	
Date:	March 5, 2020

1.2 Table of Contents

1.0 Section 5: Vendor Proposal 1-1
1.1 Title Page 1-3
1.2 Table of Contents 1-5
1.3 Certification and Signature Page (Section 3) and Other Required Forms 1-7
1.4 Executive Summary 1-39
1.5 Proposed Clarifications and Exception Requests 1-45
2.0 Attachment 3: Vendor Qualifications and Experience 2-1
FDGS Experience: Our EVV Story 2-1
2.1 Organization Overview 2-2
2.2 Mandatory Qualifications 2-4
2.3 Existing Business Relationships with the State 2-5
2.4 Business Disputes 2-6
2.5 References 2-7
2.6 Financial Stability 2-24
3.0 Attachment 4: Project Organization and Staffing Approach 3-1
3.1 Initial Staffing Plan 3-2
3.2 Key Staff, Resumes, and References 3-11
4.0 Attachment 5: Initial Work Plan 4-1
4.1 Initial Work Plan Attachment 4-10
4.2 Abridged Project Management Plan 4-19
5.0 Attachment 6: Mandatory Requirements 5-1
5.1 Completed Attachment 6: Mandatory Requirements 5-9
6.0 Attachment 7: Business Specifications Approach 6-1
6.1 Visit Verification 6-4
6.2 Program Management 6-17
6.3 Program Integrity 6-23
7.0 Attachment 8: Technical Specifications Approach 7-1
7.1 Data Sources, Delivery, and Display 7-4
7.2 Data Quality 7-21
7.3 Hardware and Infrastructure 7-28
7.4 Security Management 7-38

8.0 Attachment 9: Implementation Specifications Approach 8-1
8.1 Project Management Methodology 8-3
8.2 Implementation Methodology 8-29
8.3 Deployment Methodology 8-37
8.4 Training 8-39
8.5 CMS Certification 8-48
9.0 Attachment 10: Maintenance & Operations Specifications Approach 9-1
9.1 Operations 9-1
9.2 Solution Backup, Disaster Recovery, and Failover 9-12
10.0 Appendix 1: Detailed Specifications 10-1
10.1 Completed Appendix 1: Detailed Specifications 10-2

1.3 Certification and Signature Page (Section 3) and Other Required Forms

RFP Section 5.3.4 & Section 7, pp. 69, 80, Section 3 and Addendum 6, Q053.

Certification and Signature Page: The Vendor should include Section 7: Certification and Signature Page, completed and signed by an authorized signatory legally binding the Vendor and include it in the labeled "Original Proposal."

First Data Government Solutions, LP (FDGS) attests and provides a completed and signed Certification and Signature Page and other required forms on the following pages. Required forms that follow include:

- Addendum Acknowledgement Form
- Addendum #7 CRFP Form
- Designated Contact/Certification and Signature Form from Section 3
- Purchasing Affidavit
- Disclosure of Interested Parties to Contracts

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP 0511 BMS2000000001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[X]	Addendum No. 1	[X]	Addendum No. 6
[X]	Addendum No. 2	[X]	Addendum No. 7
[X]	Addendum No. 3	[ ]	Addendum No. 8
[X]	Addendum No. 4	[ ]	Addendum No. 9
[X]	Addendum No. 5	[ ]	Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

First Data Government Solutions, LP
Company

Authorized Signature

March 6, 2020
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Proposal
34 — Service - Prof

Proc Folder: 623121

Doc Description: Addendum #7 Electronic Visit Verification(EVV) RFP

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2020-03-06	2020-03-12 13:30:00	CRFP 0511 BMS2000000001	8

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Name, Address and Telephone Number:

First Data Government Solutions, LP
5565 Glenridge Connector NE
Atlanta, GA 30342
Tel. 404-890-2080, Fax 402-315-5105

FOR INFORMATION CONTACT THE BUYER

Brittany E Ingraham
(304) 558-0067
brittany.e.ingraham@wv.gov

Signature X [signature] **FEIN #** 59-2582959 **DATE** March 6, 2020

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION:
Addendum No. 7 is issued to:

1. Provide Agency response to additional Vendor question.

Bid opening remains 3/12/2020 at 1:30 PM ET.

No other changes.

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Implementation-Payment Milestones				

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :

Implementation-Payment Milestones (DDI)

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Implementation-Project Management Recurring				

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :

Implementation-Project Management Recurring (DDI)

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Implementation-Training and Meeting				

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :
Implementation-Training and Meeting(DDI)

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Base Year One Operations (6 months)				

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :
Base Year One Operations (6 months)

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
5	Base Year One Operations (6 months) Additional Services	2000.00000	HOUR		

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :

Base Year One Operations (6 months) Additional Services
from 07/01/2020-12/31/2020

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
6	Base Year Two Operations				

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :

Base Year Two Operations

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
7	Base Year Two Operations Additional Services	4000.00000	HOUR		

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :

Base Year Two Operations Additional Services
from 01/01/2021-12/31/2021

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
8	Base Year Three Operations				

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :
Base Year Three Operations

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
9	Base Year Three Operations Additional Services	4000.00000	HOUR		

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :
Base Year Three Operations Additional Services
from 01/01/2022-12/31/2022

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
10	Base Year Four Operations				

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :
Base Year Four Operations

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
11	Base Year Four Operations Additional Services	4000.00000	HOUR		

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :
Base Year Four Operations Additional Services
from 01/01/2023-12/31/2023

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
12	Base Year Five Operations				

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :
Base Year Five Operations

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
13	Base Year Five Operations Additional Services	4000.00000	HOUR		

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :

Base Year Four Operations Additional Services
from 01/01/2024-12/31/2024

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
14	Optional Renewal Year One Operations				

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :

Optional Renewal Year One Operations

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
15	Optional Renewal Year One Operations-Additional Services	4000.00000	HOUR		

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :

Optional Renewal Year One Operations-Additional Services
from 01/01/2025-12/31/2025

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
16	Optional Renewal Year Two Operations				

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :

Optional Renewal Year Two Operations

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
17	Optional Renewal Year Two Operations-Additional Services	4000.00000	HOUR		

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :

Optional Renewal Year One Operations-Additional Services
from 01/01/2026-12/31/2026

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
18	Optional Renewal Year Three Operations				

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :

Optional Renewal Year Three Operations

INVOICE TO	SHIP TO
PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV25301-3709 US	PROCUREMENT OFFICER - 304-356-4861 HEALTH AND HUMAN RESOURCES BUREAU FOR MEDICAL SERVICES 350 CAPITOL ST, RM 251 CHARLESTON WV 25301-3709 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
19	Optional Renewal Year Three Operations-Additional Services	4000.00000	HOUR		

Comm Code	Manufacturer	Specification	Model #
93151507			

Extended Description :

Optional Renewal Year One Operations-Additional Services from 01/01/2027-12/31/2027

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Prebid Meeting	2019-12-16
2	Questions Due	2019-12-23

ADDITIONAL TERMS AND CONDITIONS

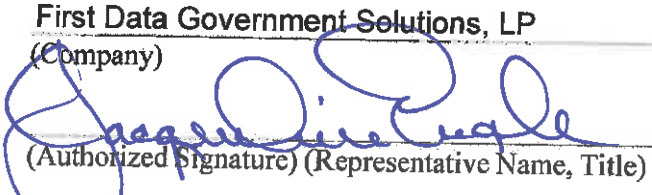
See attached document(s) for additional Terms and Conditions

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

Grant McKay, Account Executive
(Name, Title)
Grant McKay, Account Executive
(Printed Name and Title)
11311 Cornell Park Drive, Suite 300, Cincinnati, OH 45242
(Address)
513-878-8325/ 513-489-9521
(Phone Number) / (Fax Number)
Grant.McKay@Fiserv.com
(email address)

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that I have reviewed this Solicitation in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

First Data Government Solutions, LP
(Company)



(Authorized Signature) (Representative Name, Title)

Jacqueline Engle, Vice President
(Printed Name and Title of Authorized Representative)

March 5, 2020
(Date)

513-878-8123 / 402-315-5105
(Phone Number) (Fax Number)

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

CONSTRUCTION CONTRACTS: Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

ALL CONTRACTS: Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (*W. Va. Code* §61-5-3) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: First Data Government Solutions, LP

Authorized Signature: Jacqueline Engle Date: 03.05.2020

State of Ohio

County of Hamilton, to-wit:

Taken, subscribed, and sworn to before me this 5th day of March, 20 20.

My Commission expires N/A, 20___.

AFFIX SEAL HERE

NOTARIAL SEAL
STATE OF OHIO

JASON M. NELSON
Attorney at Law
Notary Public, State of Ohio
My Commission Has No Expiration
Date Section 147.03 O.R.C.

NOTARY PUBLIC Jason M. Nelson

West Virginia Ethics Commission

Disclosure of Interested Parties to Contracts

Pursuant to *W. Va. Code* § 6D-1-2, a state agency may not enter into a contract, or a series of related contracts, that has/have an actual or estimated value of $1 million or more until the business entity submits to the contracting state agency a Disclosure of Interested Parties to the applicable contract. In addition, the business entity awarded a contract is obligated to submit a supplemental Disclosure of Interested Parties reflecting any new or differing interested parties to the contract within 30 days following the completion or termination of the applicable contract.

For purposes of complying with these requirements, the following definitions apply:

"Business entity" means any entity recognized by law through which business is conducted, including a sole proprietorship, partnership or corporation, but does not include publicly traded companies listed on a national or international stock exchange.

"Interested party" or *"Interested parties"* means:

(1) A business entity performing work or service pursuant to, or in furtherance of, the applicable contract, including specifically sub-contractors;
(2) the person(s) who have an ownership interest equal to or greater than 25% in the business entity performing work or service pursuant to, or in furtherance of, the applicable contract. (This subdivision does not apply to a publicly traded company); and
(3) the person or business entity, if any, that served as a compensated broker or intermediary to actively facilitate the applicable contract or negotiated the terms of the applicable contract with the state agency. (This subdivision does not apply to persons or business entities performing legal services related to the negotiation or drafting of the applicable contract.)

"State agency" means a board, commission, office, department or other agency in the executive, judicial or legislative branch of state government, including publicly funded institutions of higher education: Provided, that for purposes of W. Va. Code § 6D-1-2, the West Virginia Investment Management Board shall not be deemed a state agency nor subject to the requirements of that provision.

The contracting business entity must complete this form and submit it to the contracting state agency prior to contract award and to complete another form within 30 days of contract completion or termination.

This form was created by the State of West Virginia Ethics Commission, 210 Brooks Street, Suite 300, Charleston, WV 25301-1804. Telephone: (304)558-0664; fax: (304)558-2169; e-mail: ethics@wv.gov; website: www.ethics.wv.gov.

Revised June 8, 2018

West Virginia Ethics Commission

Disclosure of Interested Parties to Contracts

(Required by *W. Va. Code* § 6D-1-2)

Name of Contracting Business Entity: First Data Government Solutions, LP **Address:** 5565 Glenridge Connector NE Atlanta, GA 30342

Name of Authorized Agent: Jacqueline Engle **Address:** See above

Contract Number: RFP CRFP 0511 BMS2000000001 **Contract Description:** Electronic Visit Verification Solution

Governmental agency awarding contract: WV Department of Health and Human Resources

☐ **Check here if this is a Supplemental Disclosure**

List the Names of Interested Parties to the contract which are known or reasonably anticipated by the contracting business entity for each category below *(attach additional pages if necessary)*:

1. **Subcontractors or other entities performing work or service under the Contract**
   ☑ Check here if none, otherwise list entity/individual names below.

2. **Any person or entity who owns 25% or more of contracting entity (not applicable to publicly traded entities)**
   ☑ Check here if none, otherwise list entity/individual names below.

3. **Any person or entity that facilitated, or negotiated the terms of, the applicable contract (excluding legal services related to the negotiation or drafting of the applicable contract)**
   ☑ Check here if none, otherwise list entity/individual names below.

Signature: Jacqueline Engle Date Signed: 3.5.2020

Notary Verification

State of Ohio, County of Hamilton:

I, Jacqueline Engle, the authorized agent of the contracting business entity listed above, being duly sworn, acknowledge that the Disclosure herein is being made under oath and under the penalty of perjury.

Taken, sworn to and subscribed before me this 5th day of March, 2020.

Jason M. Nelson
Notary Public's Signature

To be completed by State Agency:

Date Received by State Agency: _____

Date submitted to Ethics Commission: _____

Governmental agency submitting Disclosure: _____

NOTARIAL SEAL STATE OF OHIO

JASON M. NELSON
Attorney at Law
Notary Public, State of Ohio
My Commission Has No Expiration
Date Section 147.03 O.R.C.

Revised June 8, 2018

1.4 Executive Summary

RFP Section 5.3.5, p. 69
Executive Summary: Provide a high-level summary of the Vendor's response and proposed solution.

FDGS is pleased to offer our industry-leading EVV solution, AuthentiCare®. AuthentiCare will provide the West Virginia Department of Health and Human Resources (DHHR), its providers, and beneficiaries with a secure, flexible, and compliant solution. Our AuthentiCare solution for EVV is now implemented in 10 different states with 7 of those as statewide EVV solutions.

Our teams have provided EVV program expertise with AuthentiCare since our earliest deployment for the State of South Carolina in 2003. The South Carolina Department of Health & Human Services continues to contract with us and awarded FDGS the most recent re-bid of its EVV system.



AuthentiCare offers the Department an EVV solution that is ready to quickly meet the upcoming deadlines for compliance with the 21st Century Cures Act in January 2021 and the subsequent CMS certification under the latest Outcomes Based Certification (OBC) process. To meet these quickly approaching deadlines, FDGS closely examined the RFP requirements in discussion with our CMS and EVV subject matter experts to develop our solution and implementation approach.

To achieve the immediate needs of the Department for its EVV solution and meet the 21st Century Cures Act deadline of January 1, 2021, we have developed the best solution that proposes a focused approach to Go Live. Our approach provides an intense focus on only those business and technical specifications necessary to:

1. Verify and validate all EVV capabilities are included to fully comply with the 21st Century Cures Act
2. Include all requirements and capabilities needed to certify West Virginia's EVV solution CMS according to their Outcomes Based Certification guidelines and processes

With this focused approach to the initial implementation period, FDGS will work with the Department to validate all requirements necessary for Go Live according to the priority business and technical specifications, iteratively complete the design and configuration specific to West Virginia's program policy, and deploy a fully functional EVV solution to meet Cures Act compliance and prepare the Department for the CMS certification steps.

Upon award, FDGS will lay out an initial plan for proposed future releases to include the additional features and functions necessary to support the remaining requirements noted as "Will Meet" in Appendix 1 – Detailed Specifications.

AuthentiCare's Proven Success with DXC Integration

Currently, AuthentiCare is integrated with various vendor-managed MMIS systems in each of our EVV projects. AuthentiCare has been integrated with DXC-based MMIS platforms similar to

West Virginia's in Oklahoma, Kansas, Alabama, and Nevada. Our experience with DXC platform integration reduces both the risk and required timeframe to implement.

Some MMIS claim processing statistics are included below from our integration with DXC/interChange systems. FDGS can provide additional integration and interface statistics from other agencies upon request or during the vendor presentation.

- **Oklahoma** (DXC/interChange): Since beginning our operation in 2009, 4 million claims have been processed annually for more than 300 provider locations and 26,000 beneficiaries. ***99.5 percent*** of first-pass submitted claims were transmitted and paid via an 837 specification compliant file to the DXC MMIS portal.
- **Kansas** (DXC/interChange): Since 2010, 4 million claims have been processed annually for more than 600 provider locations and 21,000 beneficiaries. ***99.3 percent*** of submitted claims were transmitted via an 837 specification compliant file to the DXC MMIS portal for adjudication.
- **Alabama** (DXC/interChange): AuthentiCare went live on October 2017. Since then, over 5 million claims have been processed, and 837 and 835 files are being exchanged via secure File Gateway with the DXC operated and managed MMIS system. ***98.9 percent*** of claims submitted to the DXC MMIS portal are successfully paid.

Clear Benefits to States, Providers, Agencies, and Members

As DHHR evaluates proposals for EVV solutions, FDGS recommends that focusing on the long-term benefits of EVV to the State, the provider community, agencies, members, and direct care workers.

Based on our experience, we recommend that your EVV vendor provide benefits—like tangible savings, client well-being, and program quality—through its comprehensive design as well as scalable and configurable technology provided to the State and all of its EVV stakeholders. AuthentiCare can provide all of these benefits to West Virginia as its EVV solution.

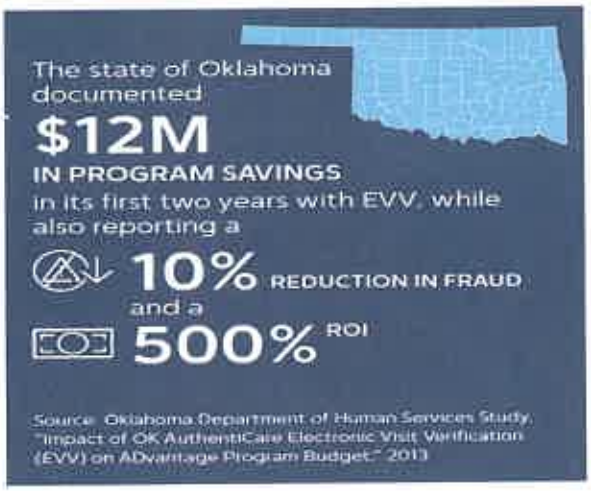


Figure 1.1 – AuthentiCare provides significant ROI for our customers

Our EVV solution has resulted in reduced and avoided costs associated with fraud, waste, and abuse. The State of Oklahoma has documented approximately $12 million in program savings in just the first two years of operation. At the same time, it realized at least a 10 percent reduction in fraud and a 500 percent return on investment (ROI).

Table 1.1 describes the benefits to the State of implementing EVV, while Table 1.2 offers information about the benefits to providers.

Table 1.1 – EVV Benefits for the State

Benefit to State	How Does this Help?
Maintain full Medicaid funding by complying with 21st Century Cures Act mandate	Avoid penalties for non-compliance with the 21st Century Cures Act.
Federal funding for 90% of implementation and 75% of operating cost	Very low proportional investment required from the state.
Pay only for services actually delivered; pay only for full duration of visit	Typical savings of 4 to 5 percent of Medicaid home care spending from not paying for missed services or foreshortened visits. Serve more people and an aging population with same amount of funding.
Reduce Nursing Home utilization	Typical savings of 30 percent by caring for a client at home or day facility, but varies greatly by individual.
Transparent records deter and reduce waste and fraud.	Additional savings, but varies by program and strength of existing controls.
Full audit trail of services	Better visibility leads to better management of recipient care.
Better data-driven management of waiver and state programs	Real data is available to identify best practices and optimize care.

Table 1.2 – EVV Benefits to Providers and Agencies

Benefit to Providers and Agencies	How Does this Help?
Automates scheduling and managing service delivery **Eliminates time sheets and time sheet processing**	Particularly valuable option for scheduling and service delivery for small and medium-sized provider agencies that cannot invest in more extensive automation.
Service location captured in real time **Alerts for late or missed scheduled visits** **Service dashboards to identify issues and address**	Puts real-time management and deployment of workers online for providers. Includes geo-fencing with state-defined rules for acceptance, exception/suspense, or rejection of visits made outside of a recipient's stored locations for care delivery.
Automated service billing: provider simply edits and approves	Eliminates service bureau per-claim submission charges.
Automates plan of care activity checklist **Collects observations of recipient care**	Reduces administrative paperwork for provider agencies. Verifies that clients are receiving appropriate care and follow up.
Fast, on-time payment (usually the next payment cycle) **Manages exceptions and tracks payments** **Integrates with back-end office and payroll systems**	Speeds reimbursement cash flow. Automates claim and payment processes to optimize cash flow while ensuring claims are validated against business rules and authorizations. Simplifies provider payroll with system output commonly used for provider payroll processing.

The Solution for West Virginia DHHR

From the RFP, we understand the State of West Virginia wishes to procure an Electronic Visit Verification (EVV) solution including data aggregation services. The EVV solution must quickly become compliant with the 21st Century Cures Act.

AuthentiCare provides the Department with a flexible, role-based, hosted EVV system, providing secure HIPAA, HITECH, and NIST-compliant identification, authentication, and authorization, and real-time data feeds with the ability for providers and payers to manage their own users.

Our EVV solution already supports the Cures Act requirements with a flexible and highly configurable framework to meet the specific EVV program and policy business processes in West Virginia.

Benefits of the AuthentiCare solution for EVV

- ✓ Fully compliant with the 21st Century Cures Act
- ✓ Flexible and highly configurable framework
- ✓ Scalable solution for high volumes of visits anytime, anywhere
- ✓ Complete Data Aggregation services
- ✓ Automated claims processing via standard data interchange technology
- ✓ Reduced Medicaid costs due to reduced potential for fraud, waste, and abuse

AuthentiCare offers clear benefits to both large and small providers. For large providers, AuthentiCare supports system automation and large volume data extracts including visit data. AuthentiCare allows an input to their back office systems to generate worker payroll and track accounts receivable. For the smaller providers, AuthentiCare will greatly reduce, if not eliminate paper and manual processes. For example, AuthentiCare offers automated scheduling, real-time dashboards for status updates, and automated billing tied directly to the verification.

Innovative Mobile Approach

Our most innovative features are provided through our AuthentiCare Mobile application, providing flexibility for continuous collection of visit information in rural West Virginia locations that may not have cellular connectivity. The mobile app has two modes for connectivity for caregivers: Standard and Frontier. Workers can use the mode that best fits the connectivity options in their area. Frontier mode overcomes connectivity issues found in rural areas.

Workers install the free mobile app on their own phone or tablet and use it to check in and check out when providing care. The system uses the device's network time and GPS location to verify the start and end times of the visit and the location of service in real-time. Visit information is stored on the device until the worker has Wi-Fi or cellular data coverage, and then the data is automatically uploaded, making this a paperless solution.

In limited service areas, the AuthentiCare mobile application provides Store and Forward technology features. In contrast to other vendors, the AuthentiCare Store and Forward solution uses the mobile network time and GPS location services for EVV, rendering a fixed device unnecessary.

Expertise with CMS Standards and Certification

CMS considers the AuthentiCare EVV solution to be a Medicaid enterprise module and a candidate for certification to qualify for enhanced funding for DDI and M&O phases. In addition

to our EVV program knowledge and leadership, FDGS is currently an IV&V vendor for an EVV implementation project starting up with the Outcomes Based Certification (OBC) process. We are actively working with three of our AuthentiCare customers on OBC: with Nevada Department of Health Care and Finance Policy we are in process with OBC, with Oklahoma Department of Human Services we are initiating the OBC process, and with Kansas Department of Aging and Disability Services we are in OBC planning.

CMS Certification is not just a one-time event. The new EVV OBC approach requires a State Medicaid Agency to report quarterly on Key Performance Indicators (KPIs) and provide an annual security and privacy KPI report. The KPI reports are mandatory for DHHR to continue receiving the Maintenance and Operations enhanced funding. FDGS is aware that the Department maintains a focus and level of rigor around information technology—clearly shown by its MITA 3.0 certification and the completion of the HITECH component. FDGS' approach and capabilities provide DHHR with the confidence that our AuthentiCare EVV solution meets federal requirements for certification and the ongoing compliance for M&O enhanced federal funding.

Our proposed AuthentiCare implementation team includes a CMS Certification SME as an integral resource. Our Certification SMEs have extensive knowledge of CMS certification processes including:

- Experience and knowledge into the new Outcomes Based Certification (OBC) processes
- Medicaid Enterprise Systems
- MITA architecture
- EVV solutions

FDGS has been working with CMS and the State of Nevada DHCFP prior to the official release of the new EVV OBC certification process in October 2019. Our OBC certification work in Nevada and with other customers enables us to offer DHHR a ***successful path to CMS certification*** of its EVV solution.

Summary

We look forward to the opportunity to partner with the State of West Virginia to quickly achieve compliance with the 21st Century Cures Act and attain CMS certification of the EVV system through a phased implementation approach. The AuthentiCare EVV solution from FDGS includes:

- The most statewide EVV deployments, providing real-world experience and expertise
- An EVV solution that already meets the requirements for 21st Century Cures Act compliance
- Working knowledge executing within the new CMS certification processes, minimizing the risk associated with another vendor
- Fully hosted EVV solution within our world-class data centers for the highest level of security and privacy protection
- Cost-effective EVV solution with proven short-term ROI

1.5 Proposed Clarifications and Exception Requests

First Data Government Solutions, LP (**First Data** or **FDGS**) submits its response to the Request for Proposal subject to the following exceptions made to the RFP documents identified below. In the event First Data is awarded the Project by the State of West Virginia Department of Health and Human Resources Bureau for Medical Services (**DHHR** or **State**), FDGS welcomes the opportunity to enter into good faith negotiations with the State towards the execution of a mutually acceptable definitive agreement between the parties to govern the awarded services.

Table 1.3 – Proposed Exceptions

Paragraph # and Page	Current Language	Proposed Exception with Alternative Language
RFP 22 of 229	**27. ASSIGNMENT:** Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.	FDGS requests an exception to the State's assignment language requirements listed in the RFP response section column and ask that, if awarded the Project, FDGS has the ability to enter into good faith negotiations to modify the language as follows: "**27. ASSIGNMENT:** Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments. Notwithstanding the foregoing, such prior written consent of an assignment may be waived where the assignment is due to a sale, reorganization, merger or consolidation of Vendor's business entity or parent company."
RFP 25 of 229	**41. BACKGROUND CHECK**: In accordance with W. Va. Code § 15-2D-3, the Director of the Division of Protective Services shall require any service provider whose employees are regularly employed on the grounds or in the buildings of the Capitol complex or who have access to sensitive or critical information to submit to a fingerprint-based state and federal background inquiry through the state repository. The service provider is responsible for any costs associated with the fingerprint-based state and federal background inquiry. After the contract for such services has been approved, but before any such employees are permitted to be on the grounds or in the buildings of the Capitol complex or have access to sensitive or critical information, the service provider shall submit a list of all persons who will be physically present and working at the Capitol complex to the	FDGS will comply with the State's requirements listed in the RFP response section column; provided, however, if awarded the Project, FDGS request that the State allow for the following clarification language to be inserted into this section to exclude the following Vendor personnel from the scope of the State's background check requirements: "For clarity and for avoidance of doubt, the fingerprint-based state and federal background inquiry requirements shall not apply to Vendor's employees and contractors that provide maintenance and support services in Vendor's shared services and multi-tenant data center environment."

Paragraph # and Page	Current Language	Proposed Exception with Alternative Language
	Director of the Division of Protective Services for purposes of verifying compliance with this provision. The State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check.	
Appendix 1 – Detailed Specifications	**Req ID: OP033**: The Vendor should submit the annual Statement on Standards for Attestation Engagements, System, and Organization Controls (SOC) 1, Type II audit report, using the most current version of the audit, to the Department for approval with an action plan to remediate findings within a timeframe agreed upon by the Vendor and the Department.	FDGS requests an exception to the State's requirements listed in the RFP response section column. FDGS cannot agree to the State having the ability to make decisions on policies, processes and procedures that impact FDGS' customers on an enterprise-wide basis. If awarded the Project by the State, FDGS requests the following modification be made to the State's requirements: "The Vendor should submit the annual Statement on Standards for Attestation Engagements, System, and Organization Controls (SOC) 1, Type II audit report, using the most current version of the audit, to the Department. ~~for approval with an action plan to remediate findings within a timeframe agreed upon by the Vendor and the Department.~~"

Table 1.4 – Proposed Clarification

Paragraph # and Page	Current Language	Clarification with Alternative Language
Appendix 1 – Detailed Specifications	**Req ID: SM058:** The Vendor should supply, on an annual basis, a report of the results of all security, privacy, and risk assessments, including all tools used, and an action plan detailing the approach for remediation of security risk vulnerabilities. Data and testing results, including reports, should be retained for 10 years per CMS guidelines.	FDGS agrees to commit to meeting the CMS guidelines for data retention and asks that the requirement be modified to reflect the CMS requirement as follows: **"Req ID: SM058:** The Vendor should supply, on an annual basis, a report of the results of all security, privacy, and risk assessments, including all tools used, and an action plan detailing the approach for remediation of security risk vulnerabilities. Data and testing results, including reports, should be retained for ~~10~~ 6 years per CMS guidelines."

2.0 Attachment 3: Vendor Qualifications and Experience

RFP Section 5.4.2.10 (Table 11) & Attachment 3, pp. 73, 98
1.1 The Vendor's Technical Proposal should include: organization overview, corporate background, Vendor's experience in public sector, and certifications.

FDGS has been providing Electronic Visit Verification solutions to state agencies and managed care organizations since 2002.

FDGS has worked in the health and human services arena since 1989, providing assistance to state government organizations as they modernize their legacy systems, optimize processes, and improve program delivery. Our teams have provided consulting services for over 70 government healthcare and Medicaid projects across the full spectrum of state and federal health and human services agencies. FDGS brings more than 17 years of knowledge and experience providing EVV services in the Home and Community Based Services (HCBS) sector.

FDGS Experience: Our EVV Story

FDGS Qualifications for Providing the Services Described in this RFP

FDGS has developed and operated EVV solutions for more than 17 years in the HCBS sector, addressing payment accuracy, enhancing program integrity, and improving quality of care. FDGS is a leader in this industry, having successfully implemented AuthentiCare for multiple states in programs using fee-for-service and managed care, provider and consumer-directed service delivery, and various disbursement strategies integrated with diverse fiscal agents.

In addition to a seasoned staff of government professionals, FDGS offers DHHR substantial knowledge and experience in effective provider outreach, training, and attendant enrollment. We bring our proven provider interaction methods and experiences to your implementation, supporting DHHR in strengthening its relationship with the provider community. FDGS understands that the success of your implementation is based on the solution benefits of AuthentiCare, as well as an acceptance of program change from the provider community. AuthentiCare is unique in its ability to provide benefits to all vested parties in the delivery of service: providers, consumers, and administrators. These solution services, along with our experienced help desk staff, are essential to a successful implementation and provider acceptance.

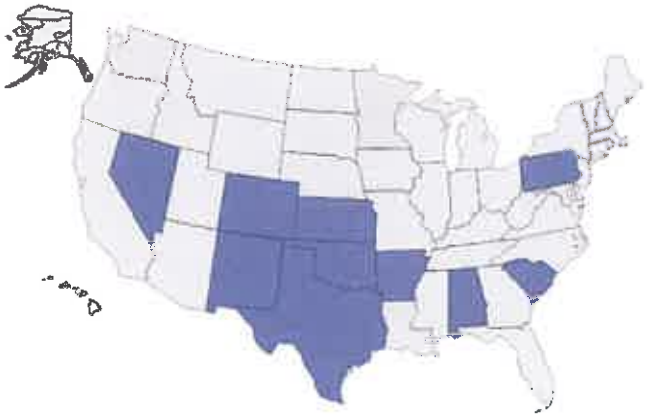


Figure 2.1 – Current AuthentiCare clients

Our EVV story began in 2002 in South Carolina with the design and development of the first Medicaid EVV solution under an APD grant from CMS that employed an Interactive Voice Response (IVR) solution to verify and document services provided in beneficiaries' homes. This experience led to development of our EVV product solution: AuthentiCare®. FDGS has enhanced the solution based on client feedback throughout the

years, adding mobile verification capabilities, enhanced system reporting, data aggregation, and certification support. AuthentiCare has now been deployed successfully statewide in Oklahoma, Kansas, New Mexico, Nevada, Texas, and Alabama, as well as continued operations in South Carolina and at WJB Dorn VA Medical Center. Additionally, we operate EVV in a self-directed program in Arkansas, Colorado, Kansas, and Pennsylvania.

2.1 Organization Overview

RFP Section 5.4.2.10 (Table 11), Attachment 3 – 1.2.1, pp. 73, 98
1.2.1 Provide all relevant information regarding the general profile of the Vendor.
Vendors are NOT to change any of the pre-filled cells in the following tables.

FDGS provides the required vendor details in Table 2.1 (RFP Table 18: Vendor Overview).

FDGS does not propose the use of any subcontractors, therefore RFP Table 19: Subcontractor Overview is not included in our response.

Table 2.1 – FDGS Organization Details (RFP Table 18)

Vendor Overview	
Company Name	First Data Government Solutions, LP
Name of Parent Company (If Applicable)	Fiserv, Inc.
Industry (North American Industry Classification System [NAICS])	518210 – Data Processing, Hosting and Related Services
Type of Legal Entity	Limited Partnership
Company Ownership (e.g., Private/Public, Joint Venture)	Public
Number of Full-Time Employees	396 (for FDGS only) Approximately 44,000 Fiserv employees
Last Fiscal Year Company Revenue	$10,187 million (2019)
Last Fiscal Year Company Net Income	$ 914 million (2019)
% of Revenue From State and Local Government Clients in the United States	30% of FDGS revenue is State & Local (remaining 70% is from federal clients)
% of Revenue From IT Design and Implementation Services	92% of FDGS revenue is from IT Design and Implementation Services
Number of Years in Business	35 years
Number of Years Vendor has been Providing the Type of Services Specified in the request for proposal (RFP)	17 years (since 2002)
Number of Employees Providing the Type of Services Specified in the RFP	36 (primary to AuthentiCare product) 51 (shared services)
Headquarters in the United States	FDGS – Atlanta, GA Fiserv – Brookfield, WI

Locations in the United States	Multiple locations across the United States, including headquarters, plus: • Cincinnati, OH • Omaha, NE • Chandler, AZ • New York, NY • Hagerstown, MD

2.1.1 Corporate Background

Experience You Can Rely On

First Data Government Solutions, LP is a limited partnership business entity and the government-facing business component of Fiserv, a $10.2 billion Fortune 500 company.

For 35 years, Fiserv has been a leader in financial services technology. Fiserv was formed on July 31, 1984, through the combination of two major regional data processing firms located in Milwaukee, Wisconsin, and Tampa, Florida. On July 29, 2019, Fiserv (NASDAQ: FISV) and First Data closed on the transformative combination of the two companies, creating the preeminent global provider of payments and financial technology, and to redefine the way money and information moves for our clients in a rapidly changing world. First Data was the largest merchant acquirer, issuer processor, and independent network services provider in the world, enabling businesses to accept electronic payments, helping financial institutions issue credit, debit and prepaid cards; and routing secure transactions between them.

FDGS has 396 total employees and consists of various groups that support the platforms, environments, compliance, and security of government clients, including the AuthentiCare solution for EVV, Medicaid, integrated eligibility, and other Health and Human Services (HHS) programs. Furthermore, FDGS has the support of the greater Fiserv Corporation with more than 44,000 employees supporting financial, security, data center management, facilities management, and business continuity practices.

Our technical expertise spans all aspects of EVV functionality and operations. Our team has expanded its expertise to enhance the AuthentiCare EVV product suite, which now supports additional federal and state requirements, including HIPAA and HITECH standards and requirements. FDGS hosts its AuthentiCare solution in redundant data centers in Omaha, Nebraska and Chandler, Arizona.

2.1.2 Certifications

FDGS and AuthentiCare maintain the following certifications:

- ADA: AuthentiCare is accessible and compliant with ADA, Section 508 and WCAG 2.0 standards
- SSAE-18: an attestation standard related to controls at service organizations and part of the American Institute of Certified Public Accountants' (ACIPA) Service Organization Control (SOC) reporting framework
- Service Organization Control (SOC): internal control reports related to a service organization. SOC reports provide information that is used to assess and document the risks and controls associated with outsourced services

To provide effective security, members of our Cyber Security organization maintain a large number of certifications including numerous cyber security interests such as Network Defense, Penetration Testing, Incident Handling, Malware, Ethical Hacking, Digital Forensics, and Incident Response. They are responsible for creating and maintaining security policies and standards, risk management, investigations and threat management, overseeing their implementation, and validating compliance. A sample of those certifications from Global Information Assurance Certification (GIAC) and other organizations include:

- GIAC Certified Enterprise Defender
- GIAC Certified Intrusion Analyst
- GIAC Certified Incident Handler
- GIAC Continuous Monitoring Certification
- GIAC Network Penetration Testing Certification
- GIAC Security Leadership
- GIAC Web Application Penetration Testing
- Qualys Certified Specialist

2.2 Mandatory Qualifications

RFP Section 5.4.2.10 (Table 11), Attachment 3 – 2., pp. 73, 101
This section details the mandatory qualifications. The Vendor must complete this section to demonstrate that it has the experience needed to meet requirements set forth in this RFP.
2.1 Table 20: Mandatory Qualifications below lists each mandatory qualification, the Vendor must note whether it meets the qualification and provide narrative demonstrating fulfillment of the requirement.
2.2 The Vendor must list each project experience separately and completely every time it is referenced.

First Data Government Solutions, LP meets all mandatory requirements listed in RFP Table 20: Mandatory Qualifications. We have provided a brief narrative in Table 2.2 for each mandatory qualification item. We are able to provide more information for each item if DHHR requests clarification.

Table 2.2 – FDGS Meets all Mandatory Qualifications (RFP Table 20: Mandatory Qualifications)

Mandatory Qualification Item(s)	Provide a Brief Narrative to Demonstrate Fulfillment of Requirement
The Vendor must demonstrate experience within the last three (3) years as the prime contractor for at least three (3) federal, state, local government or private healthcare entities where the proposed solution of similar size and scope is currently being or has been implemented.	Since 2002, FDGS has provided consulting services for over 70 government healthcare and Medicaid projects across the full spectrum of state and federal health and human services agencies. Within the last three years, FDGS has experience as the prime contractor for seven different public and private entities where we implemented AuthentiCare for jurisdictions of similar size and scope to the project requirements of this RFP. FDGS is the prime contractor for the following EVV projects including our AuthentiCare solution with projects of similar size and scope: • State of South Carolina

Mandatory Qualification Item(s)	Provide a Brief Narrative to Demonstrate Fulfillment of Requirement
	• State of Oklahoma • State of Kansas • State of Alabama • State of New Mexico • State of Nevada • State of Texas
The Vendor must demonstrate at least three (3) years' experience in Medicaid and Health and Human Services.	Since 1989, FDGS has provided consulting services for over 70 government healthcare and Medicaid projects across the full spectrum of state and federal health and human services agencies. We have 30 years of experience in Medicaid and Health and Human Services. Refer to Proposal Section 2.5 References for demonstrated experience for at least three years' experience in Medicaid and Health and Human Services.
The Vendor must include at least three (3) references from projects performed within the last three (3) years that demonstrate the Vendor's ability to perform the scope of work described in the RFP. Vendors may only use one (1) reference per project performed. DHHR strongly prefers three (3) references from different state engagements where the proposed solution is currently or has been implemented. Note, because this item is a mandatory requirement, it will not be scored.	See Proposal Section 2.5 References where we have included 11 references from South Carolina, Texas (Accenture), Oklahoma, Kansas, Alabama, New Mexico, Arkansas (Palco), Colorado (Palco), Pennsylvania (Palco), Kansas Work (Palco), and US Veterans Affairs within the format of RFP Table 21: Vendor References. All noted references and project details are from projects where AuthentiCare is currently or was previously implemented according to project requirements similar in size and scope to those from West Virginia DHHR in this RFP.
The solution proposed by the Vendor must have been previously implemented successfully in a State environment.	The fully hosted AuthentiCare solution for EVV has been successfully implemented in seven other state environments including South Carolina, Oklahoma, Kansas, New Mexico, Nevada, and Alabama. Additionally, we are currently engaged with the State of Texas (through the Accenture contract with Texas Health and Human Services).
The Vendor must have at least three (3) years' experience in operation of the proposed solution with similar size and scope to the State's in compliance with all Federal and State regulations.	FDGS has experience in operations of AuthentiCare with similar size and scope to this RFP since 2003, providing us with more than 17 years of experience operating our proposed solution. AuthentiCare is currently operational in 10 states and complies with federal and the respective state regulations including HIPAA/HITECH, the 21st Century Cures Act, CMS certification, and NIST security and privacy guidelines.

2.3 Existing Business Relationships with the State

RFP Section 5.4.2.10 (Table 11), Attachment 3 – 3., pp. 73, 102
3.1 Describe any existing or recent (within the last five [5] years) business relationships the Vendor or any of its affiliates or proposed Subcontractors have with the State, the State's counties, and/or the State's local municipalities.

Within the past five years, First Data Government Solutions, LP has not had any business relationships with the State of West Virginia, its counties, nor any local municipalities.

2.4 Business Disputes

RFP Section 5.4.2.10 (Table 11), Attachment 3 – 4., pp. 73, 103
4.1 Provide details of any disciplinary actions and denote any that are pending litigation or Terminated for Cause or Convenience and associated reasons. Also denote any other administrative actions taken by any jurisdiction or person against the Vendor. List and summarize all judicial or administrative proceedings involving your sourcing activities, claims of unlawful employment discrimination, and anti-trust suits in which you have been a party within the last five (5) years. If the Vendor is a subsidiary, submit information for all parent companies. If Vendor uses Subcontractors, associated companies, or consultants that will be involved in any phase of this project, each of these entities will submit this information as part of the response.

First Data Government Solutions, LP (FDGS LP) has not had any terminations for default or cause within the last five years. FDGS LP has had two instances of contracts cancelled or terminated for convenience, described below.

COMPANY NAME:	New Mexico Human Services Department	
COMPANY ADDRESS: (Street, City, State, Zip Code)	1301 Siler Road, Building B/C Santa Fe, NM 87507	
CONTACT NAME/PHONE:	Mario Gonzales, Project Management Bureau Chief/(505) 476-3948	
EMAIL:	Mario.gonzales@state.nm.us	
CONTRACT AWARD DATE: October 2014	**OPERATIONS START DATE:** N/A	**OPERATIONS END DATE:** Termination for convenience – April 2016
DESCRIPTION OF SERVICE: The New Mexico Human Services Department (HSD) is the fifth-largest state agency in New Mexico with approximately 2,000 staff members in 50 office locations statewide. HSD initiated two projects—the Child Support Enforcement System Replacement (CSESR) and Medicaid Management Information System Replacement (MMISR)—to replace its legacy systems. First Data provided the procurement, project management, and quality assurance services to support HSD through the acquisition, development, and implementation periods. The State of New Mexico decided to terminate for convenience the Fixed Price PMO contract for both Medicaid and Child Support Enforcement system replacement. The State is utilizing a Time & Materials, Staff Augmentation model for the Medicaid PMO services and, due to budget constraints, is reevaluating next steps for the State's Child Support Enforcement system replacement strategy. Since this decision, First Data Government Solutions, LP continues to provide various staff augmentation services to the State of New Mexico. We currently provide services to the Medicaid Deputy Director, as well as Information Services support conducting financial analysis for MMISR, the state's Medicaid modernization project.		

COMPANY NAME:	Louisiana Department of Health and Hospitals	
COMPANY ADDRESS: (Street, City, State, Zip Code)	628 North 4th Street, Bienville Building, 7th Floor BIN24 Baton Rouge, LA 70802	
CONTACT NAME/PHONE:	Jeanne LeVelle, Medicaid Program Support/(225) 342-9846	
EMAIL:	Jeanne.levelle@la.gov	
CONTRACT AWARD DATE: October 2014	**OPERATIONS START DATE:** N/A	**OPERATIONS END DATE:** Termination for convenience – September 2015
DESCRIPTION OF SERVICE: First Data Government Solutions contracted with the State of Louisiana to implement First Data's healthcare product (AuthentiCare). The State ultimately decided not to employ AuthentiCare for its EVV services and terminated the contract for convenience so that the State could stay with its legacy vendor of 10 years.		

2.5 References

RFP Section 5.4.2.10 (Table 11), Attachment 3 – 5., pp. 73, 103
The Department of Health and Human Resources (DHHR) will conduct reference checks to verify and validate the past performance of the Vendor and its proposed Subcontractors.
5.1 Vendor (Prime) References Form
5.1.1 Include at least three (3) references from projects performed within the last three (3) years that demonstrate the Vendor's ability to perform the scope of work described in this RFP.
5.1.2 The Vendor should provide three (3) different clients/projects in order to demonstrate its experience.
5.1.3 Vendor should include project description, contract dates, and contact information (customer points of contact, addresses, telephone numbers, and email addresses).
5.1.4 The Vendor should explain whether it performed the work as a prime contractor or as a subcontractor.
5.1.5 The Vendor should provide a response using Table 21: Vendor References. The Vendor may add additional Reference Tables as necessary.

AuthentiCare provides more references than any other vendor – including multiple agencies that have chosen to maintain our long-term relationships through re-bid opportunities.

FDGS brings to DHHR experience in seven statewide implementations and a demonstrated record of operational excellence, positioning us to continue to successfully meet all the requirements in this RFP for the EVV Project. Our staff's qualifications and experience with EVV programs in a total of ten different states, our ability to bring together diverse stakeholders, and our expertise in design and implementation of large-scale projects in a government environment are directly relevant to this project.

Over the years, FDGS has continued to refine and enhance AuthentiCare, creating a dynamic, flexible product configured for each state's needs. Our investment in resources and technologies produced the AuthentiCare framework that will be leveraged in the delivery of the EVV solution for West Virginia.

FDGS has the experience and knowledge to continue to support the desired solution and the evolving needs of WV DHHR. To validate the ability of FDGS to deliver EVV solutions and services from projects of similar size and scope, we have included two contacts as references for each project (if available).

The tables below provide details for the AuthentiCare projects implemented by FDGS.

Table 2.3 – South Carolina Reference (RFP Table 21)

Vendor Information		
Vendor Name: First Data Government Solutions, LP (FDGS)	Contact Name:	Grant McKay
	Contact Phone:	513-878-8325
Customer Information		
Customer Organization: South Carolina Department of Health and Human Services	Contact Name:	Rhonda Feaster
	Contact Title:	Program Manager
Customer Address: 1801 Main Street Columbia, SC 29202	Contact Phone:	803-898-2532
	Contact Email:	Feaster@scdhhs.gov
Project Information		

Total Vendor Staff:	Six

Project Objectives: Provide EVV services statewide in South Carolina to enhance program efficiencies and ensure compliance with the 21st Century Cures Act.

Project Description: As prime contractor, FDGS provides EVV and fiscal agent services for the State of South Carolina for the Department of Disabilities and Special Needs (DDSN) and Community Long-term Care (CLTC) which includes processing:

- 6.6 million claims per year
- $156 million in claim billings per year
- 2,050 agencies and individuals serving over 20,000 recipients
- 1,780 self-directed recipients with $16.8 million in claim billings per year
- HCBS Waivers
- Consumer Directed Fiscal Agent

Vendor's Involvement: Uninterrupted operations of the AuthentiCare system. Tier 1 customer support and bi-weekly project meetings with the relationship manager and all stakeholders.

Project Benefits: State program savings and compliance with the 21st Century Cures Act.

Key Personnel

Name: Jonathan Mills	Role: Subject Matter Expert
Name: Grant McKay	Role: Subject Matter Expert
Name: Courtney Cleary	Role: Relationship Manager
Name: Jami Schurr	Role: Operations Manager

Project Measurements:

Estimated one-time costs: $0	Actual one-time costs:$0

Vendor Information

Reason(s) for change in one-time cost: Not Applicable – the AuthentiCare EVV system is currently operational so no one time costs were required

Original Value of Vendor's Contract: $2.5 Million	Actual Total Contract Value: $2.5 Million

Reason(s) for change in value: Not Applicable

Estimated Start & Completion Dates:	From:	04/2002	To:	08/2007
Actual Start & Completion Dates:	From:	04/2002	To:	Present

Reason(s) for difference between Estimated and Actual dates: Extensions in 2007 & 2012): • April 2002 – August 2007 (original contract) • August 2007 – December 2012 (Care Call rebid and extension) • December 2012 – Present (AuthentiCare)
If the Vendor performed the work as a Subcontractor, the Vendor should describe the scope of subcontracted activities: Not Applicable

Table 2.4 – Texas (Accenture) Reference (RFP Table 21)

Vendor Information		
Vendor Name: First Data Government Solutions, LP (FDGS)	Contact Name:	Grant McKay
	Contact Phone:	513-878-8325
Customer Information		
Customer Organization: Accenture (State of Texas)	Contact Name:	Chris Mayfield
	Contact Title:	Managing Director
Customer Address: 12365 Riata Trace Pkwy Austin, TX 78727	Contact Phone:	512-506-0759
	Contact Email:	Chris.R.Mayfield@tmhp.com
Project Information		
Total Vendor Staff:	Six	
Project Objectives: Provide EVV services statewide in Texas to enhance program efficiencies and ensure compliance with the 21st Century Cures Act.		
Project Description: As the prime contractor to Accenture, Texas Medicaid Management Information System (MMIS) vendor, FDGS is undergoing implementation of AuthentiCare EVV in the State of Texas. Go-live was January 2020. The solution with Accenture will include the IVR, Mobile Application, a fixed-visit verification card, and custom features based on Texas' business rules. All business rules are being verified prior to system go-live.		
Vendor's Involvement: Delivery of AuthentiCare Solution in January 2020. Support AuthentiCare through our operations team with both Account Management, Training and Call Center. Tier 1 customer support and weekly project meetings with the relationship manager and all stakeholders.		
Project Benefits: Project just went live. State program savings and compliance with the 21st Century Cures Act.		
Key Personnel		
Name: King Farias	Role: National AuthentiCare Director	
Name: Grant McKay	Role: Subject Matter Expert	
Name: Karen Brock	Role: Project Manager	
Name: Jacqueline Agnan	Role: Product Project Manager	

Name: Ari Hoffman	Role: Business Analyst			
Name: Courtney Cleary	Role: Relationship Manager			
Project Measurements:				
Estimated one-time costs: $1,000,000.00	Actual one-time costs: $1,000,000.00			
Vendor Information				
Reason(s) for change in one-time cost: Not Applicable (firm fixed price)				
Original Value of Vendor's Contract: $2,100,000	Actual Total Contract Value: $2,100,000			
Reason(s) for change in value: Not Applicable				
Estimated Start & Completion Dates:	From:	03/2019	To:	Present
Actual Start & Completion Dates:	From:	03/2019	To:	Present
Reason(s) for difference between Estimated and Actual dates: Not Applicable				
If the Vendor performed the work as a Subcontractor, the Vendor should describe the scope of subcontracted activities: Not Applicable				

Table 2.5 – Oklahoma Reference (RFP Table 21)

Vendor Information		
Vendor Name: First Data Government Solutions, LP (FDGS)	Contact Name:	Grant McKay
	Contact Phone:	513-878-8325
Customer Information		
Customer Organization: Oklahoma Department of Human Services, Aging Services Division	Contact Name:	Tim Rossi
	Contact Title:	Programs Manager
Customer Address: 6128 E. 38th Street Tulsa, OK 74120	Contact Phone:	918-933-4951
	Contact Email:	Timothy.Rossi@okdhs.org
Project Information		

Total Vendor Staff:	Four

Project Objectives: Provide EVV services statewide in Oklahoma to enhance program efficiencies and ensure compliance with the 21st Century Cures Act.

Project Description: The Oklahoma Department of Human Services contracted FDGS to provide EVV services for its Aging Services Division using the FDGS AuthentiCare solution. The Aging Services Division manages the State Plan Personal Care (SPPC) program through nursing staff located in offices throughout the State.

The Division also manages the ADvantage Home and Community Based waiver with the assistance of contracted case management providers. The combined SPPC and ADvantage programs serve approximately 25,636 individuals daily. The core service provided is personal care, which is provided in members' homes. Services are provided by a network of provider agencies that are certified by the State.

Vendor's Involvement: Implement and support an EVV system that provides monitoring of and enhanced quality of care to service recipients. Tier 1 customer support and bi-weekly project meetings with the relationship manager and all stakeholders. Work with state's MMIS provider to build an interface for file transmissions and submission of claims related data for payment.

Project Benefits: An independent study done by a third-party consultant on behalf of state of Oklahoma showed a rate of return to the state's investment in EVV to be in excess of 500 percent. Additional benefits include reduced administrative burden and operational efficiencies for provider agencies in their day to day operations.

Key Personnel

Name: Grant McKay	**Role: Relationship Manager**
Name: Gerardo Gutierrez	Role: Project Manager
Name : Jonathan Mills	Role: Subject Matter Expert
Name: Candace Cobb	Role: Training Lead

Project Measurements:

Estimated one-time costs: $0	Actual one-time costs: $0

Vendor Information

Reason(s) for change in one-time cost: Not Applicable – This is a fixed-price contract with a yearly fixed cost. There was no one-time implementation cost.

Original Value of Vendor's Contract: $3,780,000	Actual Total Contract Value: $3,780,000

Reason(s) for change in value: Not Applicable

Estimated Start & Completion Dates:	From:	07/2009	To:	Present
Actual Start & Completion Dates:	From:	07/2009	To:	Present

Reason(s) for difference between Estimated and Actual dates: We were the incumbent EVV vendor until 2015 when the state awarded the procurement to one of our competitors based on lower cost. However, the new vendor could not implement and had issues with successfully submitting claims data to the state's MMIS through the interface they built. As a result, the state went back to procurement in 2016 and we were awarded the contract again based on best value.
If the Vendor performed the work as a Subcontractor, the Vendor should describe the scope of subcontracted activities: Not Applicable

Table 2.6 – Kansas Reference (RFP Table 21)

Vendor Information		
Vendor Name: First Data Government Solutions, LP (FDGS)	Contact Name:	Grant McKay
	Contact Phone:	513-878-8325
Customer Information		
Customer Organization: Kansas Department for Aging and Disability Services (KDADS)	Contact Name:	Amy Penrod
	Contact Title:	Commissioner
Customer Address: 503 South Kansas Avenue Topeka, KS 66603	Contact Phone:	785-296-0141
	Contact Email:	Amy.Penrod1@ks.gov
Project Information		
Total Vendor Staff:	Four	
Project Objectives: Provide EVV services statewide in Kansas as prime contractor to Kansas Department of Aging and Disability Services (KDADS) and collaborate with the Managed Care Organizations (MCOs) to enhance program efficiencies and ensure compliance with the 21st Century Cures Act.		
Project Description: As prime contractor, FDGS provides EVV and monitoring services for KDADS. FDGS' EVV product, AuthentiCare, deployed for the State of Kansas currently processes: • 5 Waiver Programs • Money Follows the Person Program • 841 Providers • 19,977 Consumers • 4.5M claims annually • Mobile Application • Provide entry of authorizations through HPE from three MCOs as of January 2013 as Kansas transitioned from fee-for-service to managed care Starting 01/01/19, KanCare switched out one MCO and FDGS continues as the prime EVV vendor in the State.		
Vendor's Involvement: Implement and support an EVV system that provides monitoring of and enhanced quality of care to service recipients. Tier 1 customer support. As the prime contractor to KDADs, we also work closely with the State's Managed Care Organizations (MCOs) and providers to ensure increased quality of care through EVV to benefit recipients. We work with the State's MMIS vendor for file transmissions and submission of claims related data for payment to providers.		

Project Benefits: Reduced administrative burden and operational efficiencies for provider agencies in their day to day operations. Reduction in fraud, waste and abuse as well as state compliance with the 21st Century Cures Act requirements for EVV systems.				
Key Personnel				
Name: Grant McKay	Role: Subject Matter Expert			
Name: Asad Salahuddin	Role: Relationship Manager			
Name: Jacqueline Agnan	Role: Project Manager			
Name: Christopher Stevens	Role: Training Lead			
Project Measurements:				
Estimated one-time costs: $210,000	Actual one-time costs: $210,000			
Vendor Information				
Reason(s) for change in one-time cost: Not Applicable				
Original Value of Vendor's Contract: $805,000 Annually	Actual Total Contract Value: $805,000 Annually			
Reason(s) for change in value: Not Applicable				
Estimated Start & Completion Dates:	From:	08/2011	To:	Present
Actual Start & Completion Dates:	From:	08/2011	To:	Present
Reason(s) for difference between Estimated and Actual dates: Not Applicable				
If the Vendor performed the work as a Subcontractor, the Vendor should describe the scope of subcontracted activities: Not Applicable				

Table 2.7 – Alabama Reference (RFP Table 21)

Vendor Information		
Vendor Name: First Data Government Solutions, LP (FDGS)	Contact Name:	Grant McKay
	Contact Phone:	513-878-8325
Customer Information		
Customer Organization: Alabama Medicaid	Contact Name:	La'Quita Robinson
	Contact Title:	Associate Director, LTC Project Management/Program

Customer Address: 501 Dexter Avenue Montgomery, AL 36103	Contact Phone:	334-353-5153
	Contact Email:	LaQuita.Robinson@medicaid.alabama.gov

Project Information

Total Vendor Staff:	Five

Project Objectives: Provide EVV services to the state of Alabama to enhance program efficiencies and ensure compliance with the 21st Century Cures Act.

Project Description: As the prime contractor, FDGS provides EVV and monitoring services for the Medicaid Agency of the State of Alabama. FDGS' EVV product, AuthentiCare, currently processes:

- 6 Waiver programs managed by multiple state agencies
- 275 Providers
- 12,326 Consumers

Since system startup October 1, 2017, we have supported:

- Mobile Application
- Complex billing to state MMIS as well as state subcontractor using both 837P and 837I
- Fee for service billing on behalf of providers or state agencies, depending on waiver

Alabama Medicaid is in the process of implementing additional service types to the AuthentiCare system currently in production.

Vendor's Involvement: Uninterrupted operations of the AuthentiCare system. Tier 1 customer support and weekly operational and project meetings with the relationship manager and all stakeholders.

Project Benefits: Compliance with the 21st Century Cures Act.

Key Personnel

Name: Grant McKay	Role: Sales/Subject Matter Expert
Name: Jami Schurr	Role: Customer Trainer
Name: Courtney Cleary	Role: Relationship Manager
Name: Jim Jones	Role: Technical Support
Name: Lisa Smith	Role: Project Manager
Name: Alejandro Pessano	Role: Customer Outreach Manager

Project Measurements: We have an Operational Dashboard which tracks items such as Call Center call times, Incident, Project Plans

Estimated one-time costs: $0	Actual one-time costs:$0

Vendor Information

Reason(s) for change in one-time cost: Not Applicable

Original Value of Vendor's Contract: $400,000	Actual Total Contract Value: $412,000

Reason(s) for change in value: 1 year contract. Price is based on transaction levels.

Estimated Start & Completion Dates:	From:	01/2017	To:	Present
Actual Start & Completion Dates:	From:	01/2017	To:	Present
Reason(s) for difference between Estimated and Actual dates: Not Applicable				
If the Vendor performed the work as a Subcontractor, the Vendor should describe the scope of subcontracted activities: Not Applicable				

Table 2.8 – New Mexico Reference (RFP Table 21)

Vendor Information		
Vendor Name: First Data Government Solutions, LP (FDGS)	Contact Name:	Grant McKay
	Contact Phone:	513-878-8325
Customer Information		
Customer Organization: New Mexico Centennial Care (NMCC)	Contact Name:	Quinn Glenzinski
	Contact Title:	Director, Network Services, Government Programs
Customer Address: 5701 Balloon Fiesta Parkway Albuquerque, NM 87113	Contact Phone:	505-816-4181
	Contact Email:	Quinn_Glenzinski@bcbsnm.com
Project Information		
Total Vendor Staff:	Six	
Project Objectives: Provide EVV services statewide in New Mexico under a statewide contract with the Managed Care Organizations to enhance program efficiencies, prevent fraud, waste, and abuse and ensure compliance with the 21st Century Cures Act.		

Project Description: New Mexico Centennial Care's (NMCC) Managed Care Organizations (MCOs) contracted FDGS to implement their EVV AuthentiCare solution. The project conducted a pilot in early 2014 and since then FDGS has worked with the four original MCOs under New Mexico Centennial Care (NMCC) Waiver (1.0) and then the two remaining and one new MCOs under NMCC 2.0 and New Mexico Human Services Department to implement EVV in the entire state using a phased implementation approach. AuthentiCare EVV was fully implemented statewide as of November 13, 2016. FDGS was granted a contract extension under NMCC 2.0 procurement as the State's and MCOs EVV vendor statewide.

As the prime contractor, FDGS continues to provide EVV services for Personal Care Consumer Delegated, Personal Care Consumer Directed, Personal Care Consumer Directed Training, Respite, Supervisory Home Visit, Consumer Directed Administrative Fee, and Consumer Directed Advertisement Reimbursement Fee.

Centennial Care 2.0, which included one new MCO, took effect January 2019 and FDGS continues as sole EVV vendor in New Mexico.

- IVR, Mobile, Web, and mobile with GPS including Store and Forward technology for remote no-technology areas.
- 6 million claims created per year
- $375 million in annual claim billing
- 184 provider agencies
- 20,000 clients/beneficiaries
- 18,993 caregivers
- 5 MCOs over NMCC 1.0 and 2.0

Vendor's Involvement: Uninterrupted operations of the AuthentiCare system. Tier 1 customer support and bi-weekly project meetings with the relationship manager and all stakeholders. Additionally, the Relationship Manager also has face-to-face interaction with the Key personnel across all MCOs quarterly.

Project Benefits: State program savings, reduced administrative burden on providers, and compliance with the 21st Century Cures Act.

Key Personnel

Name: Asad Salahuddin	Relationship Manager
Name: Christopher Stevens	Project Manager
Name: Jami Schurr	Operations Manager
Name: Jonathan Mills	Subject Matter Expert
Name: Komala Nagisetty	Business Analyst
Name: Candace Cobb	Training Coordinator

Project Measurements:

Estimated one-time costs: $660,000 – one time implementation fee	Actual one-time costs: $660,000 – one time implementation fee

Vendor Information

Reason(s) for change in one-time cost: Not Applicable

Original Value of Vendor's Contract: $1,272,000	Actual Total Contract Value: $1,272,000

Reason(s) for change in value: Not Applicable

Estimated Start & Completion Dates:	From:	03/2014	To:	Present
Actual Start & Completion Dates:	From:	03/2014	To:	Present
Reason(s) for difference between Estimated and Actual dates: Not Applicable				
If the Vendor performed the work as a Subcontractor, the Vendor should describe the scope of subcontracted activities: Not Applicable				

Table 2.9 – U.S. Department of Veterans Health Administration Reference (RFP Table 21)

Vendor Information		
Vendor Name: First Data Government Solutions, LP (FDGS)	Contact Name:	Grant McKay
	Contact Phone:	513-878-8325
Customer Information		
Customer Organization: U.S. Department of Veterans Health Administration (VA)	Contact Name:	Lamar Alexander
	Contact Title:	Program Analyst
Customer Address: 6439 Garner Ferry Road Columbia, SC 29209	Contact Phone:	803-776-4000 x5106
	Contact Email:	Vassilis.Alexander@va.gov
Project Information		
Total Vendor Staff:	Four	
Project Objectives: Provide EVV services to the department of Veteran Affairs in South Carolina to enhance program efficiencies, tracking, and monitoring of services to U.S. Veterans.		
Project Description: As prime contractor, FDGS provides EVV services to William Jennings Bryan Dorn VA Medical Center (Dorn VAMC) in Columbia, South Carolina. This program provides EVV for Personal Care, Adult Day Health Care, and Respite-in-home services. Additionally, FDGS integrated with a federal clearinghouse, Change Healthcare, for 837P claims processing. This implementation is currently serving nearly 3,000 veterans.		
Vendor's Involvement: Provide system updates per request of VA DORN. Provide bi-weekly touchpoints and tier 1 operational support.		
Project Benefits: The results of a detailed case study demonstrated that the Dorn VAMC has been able to reduce administrative costs and serve more veterans under its existing budget since the implementation of AuthentiCare®. This project has expanded and is currently serving nearly 3,000 veterans after starting with fewer than 500.		
Key Personnel		
Name: Grant McKay	Role: Sales Executive/SME	

Name: Courtney Cleary	Role: Relationship Manager
Name: Jim Jones	Role: Technical Support
Name: Lisa Smith	Role: Project Manager
Project Measurements: Operational dashboards to capture call center calls, emails, and incidents created along with resolution and call times. Project plans for customer enhancements.	
Estimated one-time costs: N/A	Actual one-time costs: N/A
Vendor Information	
Reason(s) for change in one-time cost: Not Applicable	
Original Value of Vendor's Contract: $180,000 (Annually)	Actual Total Contract Value: $180,000 (Annually)
Reason(s) for change in value: Not Applicable	

Estimated Start & Completion Dates:	From:	08/2013	To:	Present
Actual Start & Completion Dates:	From:	08/2013	To:	Present

Reason(s) for difference between Estimated and Actual dates: Not Applicable
If the Vendor performed the work as a Subcontractor, the Vendor should describe the scope of subcontracted activities: Not Applicable

Table 2.10 – Palco Arkansas Reference (RFP Table 21)

Vendor Information		
Vendor Name: First Data Government Solutions, LP (FDGS)	Contact Name:	Grant McKay
	Contact Phone:	513-878-8325
Customer Information		
Customer Organization: Palco Arkansas	Contact Name:	Mark Biviano
	Contact Title:	Chief Operating Officer
Customer Address: P.O. Box 242930 Little Rock, AR 72223	Contact Phone:	501-230-5751
	Contact Email:	mark@palcofirst.com
Project Information		

Total Vendor Staff:	Three

Project Objectives: Provide EVV services to Palco in Arkansas to enhance program efficiencies, tracking and monitoring of services to Self-Directed benefit recipients.

Project Description: FDGS provides the AuthentiCare mobile solution to Palco's support counselors in the State of Arkansas. The support counselors use the mobile app to check in/out when making monthly visits to the 3,600+ clients across the state. Palco uses the AuthentiCare web site and reports to have real-time access to these activities as opposed to post-visit paper time sheet reporting. Several of the AuthentiCare reports can be used to generate payroll for the support counselors.

Vendor's Involvement: Provide an EVV solution with a mobile application with a web-services interface for importing client and authorization data. Also provide Tier 1 support and AuthentiCare suite of reports.

Project Benefits: Reduced administrative burden on support counselors and employers of record by using AuthentiCare instead of a pure paper time sheet creation and submission mechanism. Enabled faster and more accurate payments to support counselors. Reduced fraud, waste, and abuse.

Key Personnel

Name: Grant McKay	Role: Relationship Manager
Name: Kathleen Reynolds	Role: Project Manager
Name: Komala Nagisetty	Role: Business Analyst

Project Measurements:

Estimated one-time costs: 0	Actual one-time costs: 0

Vendor Information

Reason(s) for change in one-time cost: Not Applicable

Original Value of Vendor's Contract: $12,000	Actual Total Contract Value: $12,000

Reason(s) for change in value: Not Applicable

Estimated Start & Completion Dates:	From:	02/01/2019	To:	Present
Actual Start & Completion Dates:	From:	03/28/2019	To:	Present

Reason(s) for difference between Estimated and Actual dates: Contract was signed on 02/01/19. Project went live on 03/28/19.

If the Vendor performed the work as a Subcontractor, the Vendor should describe the scope of subcontracted activities: Not Applicable

Table 2.11 – Palco Colorado Reference (RFP Table 21)

Vendor Information		
Vendor Name: First Data Government Solutions, LP (FDGS)	Contact Name:	Grant McKay
	Contact Phone:	513-878-8325
Customer Information		
Customer Organization: Palco Colorado	Contact Name:	Mark Biviano
	Contact Title:	Chief Operating Officer
Customer Address: P.O. Box 242930 Little Rock, AR 72223	Contact Phone:	501-230-5751
	Contact Email:	mark@palcofirst.com
Project Information		
Total Vendor Staff:	Three	
Project Objectives: Provide EVV services to Self-Directed Benefit recipients through Palco in Colorado to enhance program efficiencies, tracking and monitoring of services.		
Project Description: FDGS provides the AuthentiCare mobile solution to Palco's care givers in the State of Colorado. The caregivers use the mobile app to check in/out when making monthly visits to the clients across the state. Palco uses the AuthentiCare web site and reports to have real-time access to these activities as opposed to post-visit paper time sheet reporting. Several of the AuthentiCare reports can be used to generate payroll for the caregivers.		
Vendor's Involvement: Provide an EVV solution with a mobile application and web portal. Implement a web-services interface for importing client and authorization data. Provide AuthentiCare suite of reports.		
Project Benefits: Reduced administrative burden employers of record by using AuthentiCare instead of a pure paper time sheet creation and submission mechanism. Enabled faster and more accurate payments to caregivers. Reduced fraud, waste, and abuse.		
Key Personnel		
Name: Asad Salahuddin	Role: Relationship Manager and SME	
Name: David Sullivan	Role: Project Manager	
Name: Adaunnis Dodson	Role: Business Analyst	
Project Measurements:		
Estimated one-time costs: 0	Actual one-time costs: 0	
Vendor Information		
Reason(s) for change in one-time cost: Not Applicable		
Original Value of Vendor's Contract: $17,712	Actual Total Contract Value: $17,712	

Reason(s) for change in value: Not Applicable				
Estimated Start & Completion Dates:	From:	04/01/2019	To:	Present
Actual Start & Completion Dates:	From:	03/28/2019	To:	Present
Reason(s) for difference between Estimated and Actual dates: Not Applicable				
If the Vendor performed the work as a Subcontractor, the Vendor should describe the scope of subcontracted activities: Not Applicable				

Table 2.12 – Palco Pennsylvania Reference (RFP Table 21)

Vendor Information		
Vendor Name: First Data Government Solutions, LP (FDGS)	Contact Name:	Grant McKay
	Contact Phone:	513-878-8325
Customer Information		
Customer Organization: Palco Pennsylvania	Contact Name:	Mark Biviano
	Contact Title:	Chief Operating Officer
Customer Address: P.O. Box 242930 Little Rock, AR 72223	Contact Phone:	501-230-5751
	Contact Email:	mark@palcofirst.com
Project Information		
Total Vendor Staff:	Three	
Project Objectives: Provide EVV services to Palco in Pennsylvania to enhance program efficiencies, tracking, and monitoring of services to Self-Directed benefit recipients.		
Project Description: FDGS provides the AuthentiCare mobile solution to self-directed beneficiaries through Palco in Pennsylvania. The caregivers use the mobile app to check in/out when making monthly visits to the clients across the state. Palco uses the AuthentiCare web site and reports to have real-time access to these activities as opposed to post-visit paper time sheet reporting. Several of the AuthentiCare reports can be used to generate payroll for the caregivers.		
Vendor's Involvement: Provide an EVV solution with a mobile application, IVR, and web portal. Implement a web-services interface for importing client and authorization data. Provide AuthentiCare suite of reports.		
Project Benefits: Reduced administrative burden for employers of record by using AuthentiCare instead of a pure paper time sheet creation and submission mechanism. Enabled faster and more accurate payments to caregivers. Reduced fraud, waste, and abuse.		
Key Personnel		

Name: Asad Salahuddin	Role: Relationship Manager and SME			
Name: David Sullivan	Role: Project Manager			
Name: Adaunnis Dodson	Role: Business Analyst			
Project Measurements:				
Estimated one-time costs: 0	Actual one-time costs: 0			
Vendor Information				
Reason(s) for change in one-time cost: Not Applicable				
Original Value of Vendor's Contract: $57,600	Actual Total Contract Value: $57,600			
Reason(s) for change in value: Not Applicable				
Estimated Start & Completion Dates:	From:	10/01/2019	To:	Present
Actual Start & Completion Dates:	From:	10/01/2019	To:	Present
Reason(s) for difference between Estimated and Actual dates: Not Applicable				
If the Vendor performed the work as a Subcontractor, the Vendor should describe the scope of subcontracted activities: Not Applicable				

Table 2.13 – Palco Kansas Work Reference (RFP Table 21)

Vendor Information		
Vendor Name: First Data Government Solutions, LP (FDGS)	Contact Name:	Grant McKay
	Contact Phone:	513-878-8325
Customer Information		
Customer Organization: Palco Kansas Work	Contact Name:	Mark Biviano
	Contact Title:	Chief Operating Officer
Customer Address:	Contact Phone:	501-230-5751

P.O. Box 242930 Little Rock, AR 72223		Contact Email:	mark@palcofirst.com

Project Information

Total Vendor Staff:	Three

Project Objectives: Provide EVV Self Directed services to Palco in Kansas to enhance program efficiencies, tracking and monitoring of services to Self-Directed benefit recipients.

Project Description: FDGS provides the AuthentiCare mobile solution to caregivers of Palco's Kansas Work self-directed program in the state of Kansas. The caregivers use the mobile application and the Interactive Voice Unit (IVR) to check in/out when making monthly visits to the clients across the state. Palco uses the AuthentiCare website and reports to have real-time access to these activities as opposed to using paper time sheets. Several of the AuthentiCare reports can be used to generate payroll for the care givers.

Vendor's Involvement: Provide an EVV solution with a mobile application, IVR, and web portal. Implement a web-services interface for importing client and authorization data. Provide AuthentiCare suite of reports.

Project Benefits: Reduced administrative burden on employers of record by using AuthentiCare instead of a pure paper time sheet creation and submission mechanism. Enabled faster and more accurate payments to caregivers. Reduced fraud, waste, and abuse.

Key Personnel

Name: Asad Salahuddin	Role: Relationship Manager and SME
Name: David Sullivan	Role: Project Manager
Name: Adaunnis Dodson	Role: Business Analyst

Project Measurements:

Estimated one-time costs: $168,750	Actual one-time costs: $168,750

Vendor Information

Reason(s) for change in one-time cost: Not Applicable

Original Value of Vendor's Contract: $6000	Actual Total Contract Value: $6000

Reason(s) for change in value: Not Applicable

Estimated Start & Completion Dates:	From:	10/01/2019	To:	Present
Actual Start & Completion Dates:	From:	10/01/2019	To:	Present

Reason(s) for difference between Estimated and Actual dates: Not Applicable

If the Vendor performed the work as a Subcontractor, the Vendor should describe the scope of subcontracted activities: Not Applicable

2.6 Financial Stability

RFP Section 5.4.2.10 (Table 11), Attachment 3 – 6., pp. 73, 108
The Vendor should provide the following components for this section:
6.1 Dun & Bradstreet (D&B) Ratings
6.1.1 1. The Vendor should provide the industry standard Dun & Bradstreet (D&B) ratings that indicate its financial strength and creditworthiness, assigned to most U.S. and Canadian firms (and some firms of other nationalities) by the U.S. firm D&B. These ratings are based on a firm's worth and composite credit appraisal. Additional information is given in credit reports (published by D&B) that contain the firm's financial statements and credit payment history.

Fiserv is a $10.2 billion Fortune 500 company. It has been named among the Fortune Magazine's World's Most Admired Companies® for six consecutive years (2014 – 2019), recognized for strength of business model, people management, social responsibility, and innovative leadership. Fiserv has 49 Fiserv U.S. offices operating in 19 states.

FDGS provides Fiserv's industry standard Dun & Bradstreet (D&B) reports on the following pages. A Dun & Bradstreet report compiles available business data to measure the creditworthiness of a company. Dun & Bradstreet reports are similar to personal credit reports for businesses and are issued by the credit reporting agency.

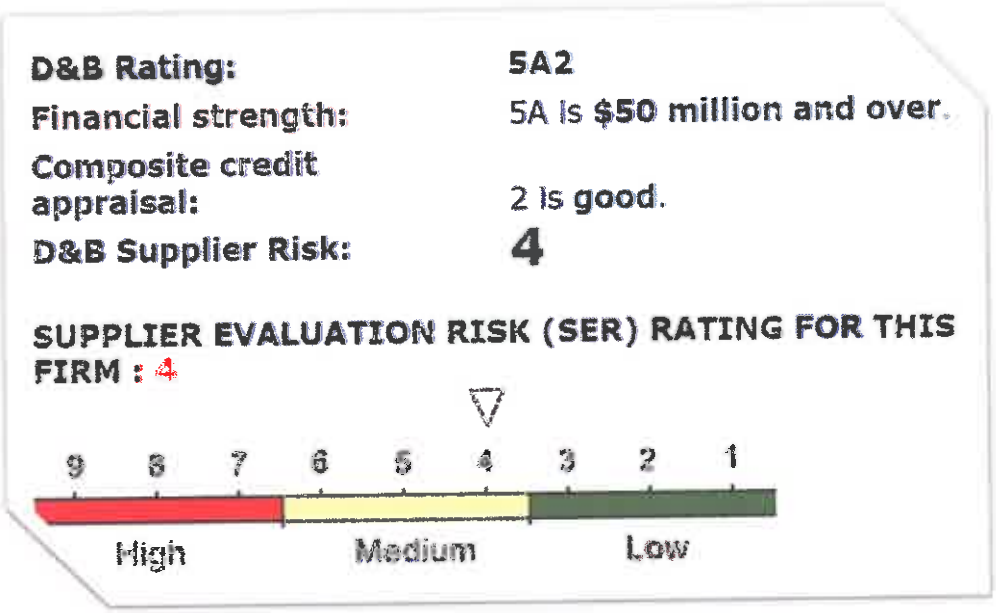


Figure 2.2 – D&B Rating Summary

FISERV, INC.

Trade Names: FISERV

ACTIVE HEADQUARTERS

D-U-N-S Number: 12-159-4832

Company: FISERV, INC.

D&B Address

Address: 255 FISERV DR
BROOKFIELD, WI, US - 53045

Location Type: HEADQUARTERS

Phone: 262-879-5000

Fax:

Web: www.fiserv.com

Added to Portfolio: 07/19/2018

Endorsement: Tammie.Neill@Fiserv.com

Last View Date: 11/05/2019

Company Summary

SCORE BAR

PAYDEX®	71	Paying 14 days past due
Commercial Credit Score Percentile	81	Low to Moderate Risk of severe payment delinquency.
Financial Stress Score National Percentile	54	Moderate Risk of severe financial stress.
D&B Viability Rating	1 5 A A	View More Details
Bankruptcy Found	N	
D&B Rating	5A2	5A indicates 50 million and over, Credit appraisal of 2 is good

D&B VIABILITY RATING SUMMARY

Viability Score

Viability Score : 1

Low Risk:1 ; High Risk:9

Portfolio Comparison

Portfolio Comparison : 5

Low Risk:1 ; High Risk:9

Data Depth Indicator

Data Depth Indicator : A

Predictive:A ; Descriptive:G

Company Profile:

A

Financial Data	Trade Payments	Company Size	Years in Business
Available	Available (3+Trade)	Large	Established

DETAILED TRADE RISK INSIGHT™

3 months from Sep-19 to Nov-19

Days Beyond Terms Past 3 months: 9 Days

Days Beyond Terms Past 3 months : 9

Low Risk:0 ; High Risk:120+

Dollar-weighted average of **153** payment experiences reported from **50** companies.

D&B COMPANY OVERVIEW

This is a headquarters location

Branch(es) or Division(s) exist
Y

Age (Year Started)
35 years (1984)

Net Worth
2293000000

Financial Condition
GOOD

Line of business
Data processing service

Gross Revenue
5823000000

Employees
24000 (65 Here)

Mailing Address
PO BOX 979
Brookfield ,WI
53008

Stock Symbol
FISV

NAICS
518210

Chief Executive
JEFFERY W YABUKI, PRES-CEO

History Status
CLEAR

Financing
SECURED

SIC
7374 ,7371

PAYDEX® TREND CHART

STOCK PERFORMANCE

FISV 105.41 0.11 ↑ (0.11%)

Previous Close:	Volume:
105.3	152,163.00
Daily High:	Daily Low:
105.82	105.16
52-Week High:	52-Week Low:
109.92	68.45
P/E:	Market Cap:
44.2857	71,623,720,898
EPS:	Div/Yield:
2.39	0.00

PUBLIC FILINGS

The following data includes both open and closed filings found in D&B's database on this company.

Record Type	Number of Records	Most Recent Filing Date
Bankruptcies	0	---
Judgments	0	---
Liens	1	01/19/2007
Suits	6	02/28/2019
UCCs	133	12/03/2018

The public record items contained herein may have been paid, terminated, vacated or released prior to today's date.

Predictive Scores

D&B VIABILITY RATING SUMMARY

The D&B Viability Rating uses D&B's proprietary analytics to compare the most predictive business risk indicators and deliver a highly reliable assessment of the probability that a company will go out of business, become dormant/inactive, or file for bankruptcy/insolvency within the next 12 months. The D&B Viability Rating is made up of 4 components:

Viability Score **Portfolio Comparison**

Compared to All US Businesses within the D&B Database:

- Level of Risk: **Low Risk**
- Businesses ranked 1 have a probability of becoming no longer viable: **0.2** %
- Percentage of businesses ranked 1: **0.3** %
- Across all US businesses, the average probability of becoming no longer viable: **14** %

Compared to All US Businesses within the same MODEL SEGMENT:

- Model Segment : **Available Financial Data**
- Level of Risk: **Moderate Risk**
- Businesses ranked 5 within this model segment have a probability of becoming no longer viable: **0.5** %
- Percentage of businesses ranked 5 with this model segment: **11** %
- Within this model segment, the average probability of becoming no longer viable: **0.6** %

Data Depth Indicator

Data Depth Indicator:

- Rich Firmographics
- Extensive Commercial Trading Activity
- Comprehensive Financial Attributes

Greater data depth can increase the precision of the D&B Viability Rating assessment.

To help improve the current data depth of this company, you can ask D&B to make a personalized request to this company on your behalf to obtain its latest financial information. To make the request, click the link below. Note, the company must be saved to a folder before the request can be made.

Request Financial Statements

Reference the FINANCIALS tab for this company to monitor the status of your request.

Company Profile:

Company Profile Details:

- Financial Data: **Available**
- Trade Payments: **Available: 3+Trade**
- Company Size: **Large: Employees:50+ or Sales: $500K+**
- Years in Business: **Established: 5+**

Financial Data	Trade Payments	Company Size	Years in Business
Available	Available: 3+Trade	Large	Established

This information may not be reproduced in whole or in part by any means of reproduction.

Disclaimer:

The software and information ("Services") accessed herein were developed exclusively at private expense, and are proprietary to Dun & Bradstreet, Inc., and its affiliates and subsidiaries (collectively, "D&B"), and may include copyrighted works, trade secrets, or other materials created by D&B at great effort and expense.

If the Customer accessing the Services is part of the executive, legislative or judicial branches of the U.S. Federal Government, the Services contained herein are a Commercial Item as that term is defined in FAR 2.101, and are comprised of Technical Data, Computer Software and Computer Software Documentation as those terms are defined in FAR 52.227-14(a) and DFAR 252.227-13.

Customer's rights to use the Services are as described in the government contract signed between D&B and the Government

Under no circumstances will the Customer accessing the Services have greater rights in the Services provided hereunder than "Limited Rights" as that term is defined in FAR 52.227-14 (ALT II) and DFAR 252.227-7013(f) and "Restricted Rights" as that term is defined in FAR 52.227-14 (ALT III) and DFAR 252.227-7014(f), respectively.

©Dun & Bradstreet, Inc. 2005-2019. All rights reserved

ONESTOP REPORT

Fiserv, Inc.

23 JULY 2019



D&B Hoovers

Table of Contents

COMPANY SUMMARY

COMPANY DESCRIPTION

PRODUCTS AND OPERATIONS

CONTACTS

CORPORATE FAMILY

CORPORATE OVERVIEW

SIGNALS

SWOT

NEWS

TRIGGERS

COMPETITORS

CLOSEST INDUSTRY PEERS

CLOSEST COMPANIES

ANALYST REPORTS

UCC FILINGS

FINANCIAL HEALTH

GEOGRAPHIC SEGMENTS

BUSINESS SEGMENTS

ANNUAL RATIOS

RATIO COMPARISONS

STOCK REPORT

ANNUAL INCOME (STANDARDIZED)

INTERIM INCOME (STANDARDIZED)

ANNUAL BALANCE (STANDARDIZED)

INTERIM BALANCE (STANDARDIZED)

ANNUAL CASH FLOW (STANDARDIZED)

INTERIM CASH FLOW (STANDARDIZED)

Company Summary

Fiserv, Inc.
255 Fiserv Dr
Brookfield, Wisconsin, 53045-5817
United States
Tel: 262-879-5000
Marketability: Has Not Opted Out of Direct Marketing
http://www.fiserv.com

Employees:	65 (This Site) 24k (All Sites)	**Fiscal Year End:**	31-Dec-2018
Company Type:	Public Parent, Headquarters	**Reporting Currency:**	USD
Corporate Family:	173 Companies	**Annual Sales:**	5.8B
Traded:	FISV (NASDAQ)	**Total Assets:**	11B
D-U-N-S® Number:	12-159-4832	**Market Value:**	37B
LEI Number:	GI7UBEJLXYLGR2C7GV83	**Fortune 1000 Rank:**	488

Business Description

Fiserv Inc. provides financial companies with the technology services they need to operate. The company provides core processing systems, electronic billing and payment systems, ATM management, and loan processing services to banks, thrifts, credit unions, and other financial institutions. It also provides licensed software, consulting, and other support services. Fiserv serves customers of all sizes, but its bread and butter has traditionally been small to midsized banks without in-house processing units. Other clients include insurance companies, merchants, leasing firms, and government agencies. Fiserv agreed to buy First Data, a payments processor, for $22 billion.

Source: D&B

Industry

D&B Hoovers:	Data Processing
US 8-Digit SIC:	73749902 - Data processing service

Corporate Highlights

Prescreen Score:	LOW RISK
Tradestyle:	Fiserv
D-U-N-S® Number:	121594832
EIN:	391506125
State Of Incorporation:	Wisconsin
Year Founded:	1984

Sales 1-Year Growth:	2.23%
Employees 1-Year Growth:	0%
Import/Export Status:	Imports
Plant/Facility Size (sq. ft.):	8,352
Auditor:	Deloitte & Touche LLP
Latitude:	43.035131
Longitude:	-88.140127

Financial Services Prospecting Suite

Total Balance	HIGHEST	1 Highest (1)	Lowest (5 or more)
Lease Balance	HIGHEST	1 Highest (1)	Lowest (5 or more)
Loan Propensity	HIGHEST	1 Highest (1)	Lowest (5 or more)
Line of Credit Propensity	LOWER	4 Highest (1)	Lowest (5 or more)
Lease Propensity	HIGHEST	1 Highest (1)	Lowest (5 or more)
Card Response	LOWEST	8 Highest (1)	Lowest (5 or more)

Key Contacts



Jeffery W. Yabuki
President, CEO and Director

Devin B. McGranahan
Senior Group President

Rene Salazar
Managing Director, Latin America, Caribbean and Canada



Steven Tait
Chief Sales Officer



Byron C. Vielehr
Chief Administrative Officer

News

Tech Know Bits — Jul 23, 2019
Fiserv (FISV) Set to Announce Earnings on Thursday

PYMNTS — Jul 22, 2019
PYMNTS.com

Newsroom — Jul 22, 2019
Survey of Mexico Residents Shows Banking Interactions Impact Daily Life

Milwaukee Journal Sentinel — Jul 18, 2019
Service and hospitality unionizers demand better workplace conditions from Fiserv Forum contractors

Financial Summary

As of 31-Mar-2019

Key Ratios	Company	Industry
Net Profit Margin (TTM) %	16.93	7.70
Return on Assets (TTM) %	9.06	3.28
Return on Equity (TTM) %	36.87	11.53
Current Ratio	1.11	1.11
Quick Ratio	0.73	0.44
Sales 5 Year Growth	3.88	
Debt to Equity	2.60	1.13

Stock Snapshot

As of 12-Jul-2019 (Financials in USD)

Traded: NASDAQ: FISV

Recent Price	94.51	**EPS**	2.43
52 Week High	94.89	**Price/Sales**	6.55
52 Week Low	68.45	**Price/Earnings**	38.89
Avg. Volume (mil)	3.50	**Price/Book**	15.49
Market Value (mil)	37,089.49	**Beta**	0.79

BACK TO TABLE OF CONTENTS

Company Description

Fiserv Inc. provides financial companies with the technology services they need to operate. The company provides core processing systems, electronic billing and payment systems, ATM management, and loan processing services to banks, thrifts, credit unions, and other financial institutions. It also provides licensed software, consulting, and other support services. Fiserv serves customers of all sizes, but its bread and butter has traditionally been small to midsized banks without in-house processing units. Other clients include insurance companies, merchants, leasing firms, and government agencies. Fiserv agreed to buy First Data, a payments processor, for $22 billion.

Operations

Fiserv's Payments businesses, which represent about 55% of its sales, provide financial institutions and other companies with products and services for processing electronic payments and for offering financial services through digital channels. Specific offerings include electronic bill payment and presentment services, debit and other card-based payment products and services, internet and mobile banking software and services, and other products.

Fiserv's Financial businesses, about 45% of revenue, provide banks, thrifts, and credit unions with back office-related account processing services, item processing and source capture services, loan origination and service products, cash management, and consulting services.

The company also owns a 49% stake in StoneRiver Group, made up of its former insurance services businesses.

Geographic Reach

Fiserv, based in Brookfield, Wisconsin, has data and transaction processing centers, development, item processing, and support centers in about 105 cities. The US is Fiserv's largest market, providing about 95% of revenue.

Sales and Marketing

Fiserv serves about 12,000 clients (including about 2,300 mobile banking clients) worldwide and enjoys high contract renewal rates. Banks typically avoid switching service providers because the cost and work involved in changing.

More than 2,500 financial institutions -- including banks, thrifts, credit unions, investment management firms, leasing and finance companies, retailers, merchants, mutual savings banks, and building societies -- have signed on to offer Fiserv's person-to-person payment services to their customers.

In 2018, Fiserv extended its marketing efforts by buying the naming rights to a new Milwaukee arena for 25 years. The Fiserv Forum is the home court of the Milwaukee Bucks.

Financial Performance

Fiserv served up its eighth straight year of revenue increases in 2017 with a 3% gain to $5.7 billion from 2016. Higher transaction volumes drove an increase in the company's card services business in 2017. The electronic payments business also increased with help from a higher level of EMV chip card manufacturing and personalization. Increased lending solution volumes led to an increase in financial segment revenue.

Net income jumped about 34% in 2017 to $1.2 billion on the higher revenue, giving Fiserv a 21% profit margin. The company also paid less in taxes in 2017 due to the US Tax Cuts and Jobs Act.

Cash from operations rose to $1.48 billion in 2017, a 4% increase from 2016, due to higher profit, somewhat offset by lower cash dividends from the StoneRiver joint venture and unfavorable timing of payables. Stock buybacks were about $1.2 billion each of the past two years.

Strategy

Fiserv has deployed several product suites and products for offering, managing, and processing digital and mobile financial transactions. Packages of products include Corillian, which enables institutions to add and integrate applications, such as electronic bill payment, person-to-person payments, and personal financial management tools. The Mobiliti product suite provides a variety of mobile banking and payments

services. Specific products include Messenger Center for cash management, Architect for online and mobile banking, and Notifi for real-time communication between institutions and customers.

Besides driving revenue with new products, Fiserv also seeks to maintain a handle on costs. The company has saved money by streamlining procurement and adjusting its workforce.

Mergers and Acquisitions

In 2019 Fiserv entered an agreement to acquire electronic payments processor First Data in an all-stock transaction valued at $22 billion. Following the deal's close Fiserv shareholders will own 57.5% of the combined company; First Data shareholders will have a 42.5% stake. The companies believe the deal will unite their complementary assets to create a combined company offering payments and financial services, including account processing and digital banking products; card issuer processing and network services; e-commerce; integrated payments; and First Data's Clover cloud-based point-of-sale product. The company's project revenue to rise at a faster rate and reduced costs of about $900 million over five years. Fiserv plans to refinance First Data's $17 billion in debt to shore up the combined company's balance sheet. The deal is expected to close in the second half of 2019.

Fiserv agreed in 2018 to acquire the debit card processing, ATM Managed Services, and MoneyPass network of US Bancorp's Elan Financial Services unit. The deal, valued at $690 million, would enhance Fiserv's ATM management services and add MoneyPass, a surcharge-free US network, to its service offerings.

In 2017 Fiserv acquired Online Banking Solutions Inc. (OBS) for $78 million. OBS provides secure online business banking services to financial institutions. The deal extends Fiserv's cash management, digital business banking, and secure browser capabilities for large commercial and small business clients.

Also in 2017 Fiserv acquired PCLender (mortgages), Dovetail (payments infrastructure), and Monitise (digital banking).

In 2016 Fiserv expanded its product base for community banks and credit unions after buying ACI Worldwide's consumer financial services business for $200 million.

Company Background

When First Bank System of Minneapolis bought Milwaukee-based Midland Bank in 1984, the head of Midland's data processing operation, George Dalton, bought the unit and then merged that operation with Sunshine State Systems, a newly independent Florida processing company headed by Leslie Muma. The company, renamed Fiserv, went public in 1986. It grew by providing outsourcing services to small banks and thrifts. In the 1990s, Fiserv began targeting larger clients.

But industry consolidation sometimes hurt the company, as when the 12-year term of a 1995 contract with Chase Manhattan was reduced to three after Chase and Chemical Bank merged in 1996.

BACK TO TABLE OF CONTENTS

Products & Operations

2017 Sales

	$ mil.	% of total
Payments		
Processing & services	2,476	43
Products	758	13
Financial		
Processing & services	2,347	41
Product	183	3
Adjustments	(68)	-
Total	5,696	100

Selected Subsidiaries

BillMatrix Corporation
CheckFree Corporation
CheckFreePay Corporation
Corillian Corporation
Fiserv Global Services, Inc.
Fiserv Automotive Solutions, Inc.
Fiserv CIR, Inc.
Fiserv (Europe) Limited (UK)
Information Technology, Inc.
ITI of Nebraska, Inc.
XP Systems Corp.

BACK TO TABLE OF CONTENTS

Contacts



Jeffery W. Yabuki

President, CEO and Director at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000

Devin B. McGranahan

Senior Group President at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000

Rene Salazar

Managing Director, Latin America, Caribbean and Canada at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000



Steven Tait

Chief Sales Officer at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000



Byron C. Vielehr

Chief Administrative Officer at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000



Lynn S. McCreary

Chief Legal Officer, Secretary at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000
Email: lynn.mccreary@fiservcfs.com

Robert W. Hau

Chief Financial Officer, Treasurer at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000

Kevin J. Schultz

Executive Vice President, President - International Group at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000

Patrick Davie

VP, Product Strategy, Card Services at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000

Scott Domach

VP, Digital Banking at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000

Rob Palin

GM, Canada at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000



Glenn M. Renwick

Independent Director at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000
Email: glenn.renwick@fiservcfs.com

Robert Bob

Chief Financial Officer at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000
Email: robert.bob@fiservcfs.com

Marc West

Chief Information Officer at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000
Email: marc.west@fiservcfs.com

Paul Dumas

Chief Human Resources Officer at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000
Email: paul.dumas@fiservcfs.com



Kevin P Pennington

Evp at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000
Email: kevin.pennington@fiservcfs.com

Mark Prout

Senior Vice President, Enterprise Operations at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000
Email: mark.prout@fiservcfs.com

Andres Pasantes

SVP, Sales, North America at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000
Email: andres.pasantes@fiservcfs.com

Todd Horvath

President, Bank Solutions at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000
Email: todd.horvath@fiservcfs.com

Cheryl Nash

President Of Investment Services at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000
Email: cheryl.nash@fiservcfs.com

Barb Lowman

Vice President, Professional Services at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000
Email: barb.lowman@fiservcfs.com

Chris Barnash

VP, IT Operations at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000
Email: chris.barnash@fiservcfs.com

Kelley Scheet

Vp, Application Support at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000
Email: kscheet@checkfree.com

Martin Coen

President Of Enterprise Payment Solutions at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000
Email: martin.coen@fiservcfs.com

James Cox

Evp Of Corporate Development at Fiserv, Inc.

Brookfield, Wisconsin, United States
Data Processing
Main: 262-879-5000

BACK TO TABLE OF CONTENTS

Corporate Family Report

173 Total Corporate Family Members (Note: Branches are hidden)

HQ Fiserv, Inc.
255 Fiserv Dr, Brookfield, Wisconsin, 53045-5817, United States
D-U-N-S® Number: 12-159-4832
Has Not Opted Out of Direct Marketing

- S Fiserv Clearing, Inc
  2005 Market St Ste 1200, Philadelphia, Pennsylvania, 19103-7008, United States
  D-U-N-S® Number: 10-822-8925
  Has Not Opted Out of Direct Marketing

- HQ Fiserv Global Services, Inc.
  255 Fiserv Dr, Brookfield, Wisconsin, 53045-5815, United States
  D-U-N-S® Number: 08-068-8613
  Has Not Opted Out of Direct Marketing

  - S Fiserv Costa Rica SA
    300 Metros Este Del Cenada, Heredia, Heredia, Costa Rica
    D-U-N-S® Number: 85-320-1945
    Has Not Opted Out of Direct Marketing

- S Bastogne, Inc.
  871 Coronado Center Dr, Henderson, Nevada, 89052-3977, United States
  D-U-N-S® Number: 96-284-0794
  Has Not Opted Out of Direct Marketing

- S Fiserv Personix
  19615 Russell Rd, Kent, Washington, 98032-1115, United States
  D-U-N-S® Number: 95-847-5795
  Has Not Opted Out of Direct Marketing

- HQ Checkfree Corporation
  2900 Westside Pkwy, Alpharetta, Georgia, 30004-7429, United States
  D-U-N-S® Number: 04-033-7243
  Has Not Opted Out of Direct Marketing

  - HQ Carreker Corporation
    4055 Valley View Ln Ste 800, Dallas, Texas, 75244-5070, United States
    D-U-N-S® Number: 09-993-1313
    Has Not Opted Out of Direct Marketing

    - S Carreker Corp
      3400 Players Club Pkwy Ste 200, Memphis, Tennessee, 38125-1731, United States
      D-U-N-S® Number: 13-045-0604
      Has Not Opted Out of Direct Marketing

HQ Corillian Corporation
3400 Ne John Olsen Ave, Hillsboro, Oregon, 97124-5808, United States
D-U-N-S® Number: 01-582-4626
Has Not Opted Out of Direct Marketing

HQ Corillian Payment Solutions, Inc
11600 Sunrise Valley Dr Ste 100, Reston, Virginia, 20191-1400, United States
D-U-N-S® Number: 03-751-0500
Has Not Opted Out of Direct Marketing

S Accurate Software Solutions LLC
16386 Sw 8th St, Hollywood, Florida, 33027-1075, United States
D-U-N-S® Number: 14-207-4041
Has Not Opted Out of Direct Marketing

HQ American Payment Systems, Inc.
15 Sterling Dr, Wallingford, Connecticut, 06492-1843, United States
D-U-N-S® Number: 60-898-6881
Has Not Opted Out of Direct Marketing

S Resources Trust Company
8051 E Maplewood Ave, Englewood, Colorado, 80111-4714, United States
D-U-N-S® Number: 10-569-6983
Has Not Opted Out of Direct Marketing

S Fiserv Ncsi Inc
451 Hungerford Dr Ste 408, Rockville, Maryland, 20850-4151, United States
D-U-N-S® Number: 07-781-9548
Has Not Opted Out of Direct Marketing

S Ips-Sendero Corporation
4801 E Thistle Landing Dr, Phoenix, Arizona, 85044-6459, United States
D-U-N-S® Number: 10-280-8524
Has Not Opted Out of Direct Marketing

S Checkfreepay Corporation
15 Sterling Dr, Wallingford, Connecticut, 06492-1843, United States
D-U-N-S® Number: 80-132-7144
Has Not Opted Out of Direct Marketing

HQ Fiserv UK Ltd.
Eversheds House, Manchester, M1 5ES, United Kingdom
D-U-N-S® Number: 22-300-9380
Has Not Opted Out of Direct Marketing

HQ Monitise Ltd.
Medius House, 3Rd Floor, London, W1F 8BH, United Kingdom
D-U-N-S® Number: 67-153-4324
Has Not Opted Out of Direct Marketing

(S) Monitise Americas, Inc.
3400 Ne John Olsen Ave, Hillsboro, Oregon, 97124-5808, United States
D-U-N-S® Number: 60-452-2735
Has Not Opted Out of Direct Marketing

(HQ) Monitise Group Ltd.
Medius House, 2 Sheraton Street, London, W1F 8BH, United Kingdom
D-U-N-S® Number: 34-790-4042
Has Not Opted Out of Direct Marketing

(HQ) Monitise Europe Ltd.
Eversheds House, Manchester, M1 5ES, United Kingdom
D-U-N-S® Number: 73-570-2479
Has Not Opted Out of Direct Marketing

(S) Monitise International Ltd.
Eversheds House, Manchester, M1 5ES, United Kingdom
D-U-N-S® Number: 34-755-3724
Has Not Opted Out of Direct Marketing

(S) Monitise Inc
1 Embarcadero Ctr Ste 900, San Francisco, California, 94111-3754, United States
D-U-N-S® Number: 07-828-7783
Has Not Opted Out of Direct Marketing

(S) Fiserv Tampa Inc
5802 Benjamin Center Dr Ste 105, Tampa, Florida, 33634-5297, United States
D-U-N-S® Number: 11-276-3370
Has Not Opted Out of Direct Marketing

(HQ) Fiserv Mortgage Servicing Systems Inc
3575 Moreau Ct 2, South Bend, Indiana, 46628-4320, United States
D-U-N-S® Number: 07-433-1893
Has Not Opted Out of Direct Marketing

(HQ) Fiserv Federal Systems, Inc.
255 Fiserv Dr, Brookfield, Wisconsin, 53045-5817, United States
D-U-N-S® Number: 83-135-1940
Has Not Opted Out of Direct Marketing

(HQ) Credit Union On-Line, Inc.
1601 Trapelo Rd Ste 201, Waltham, Massachusetts, 02451-7349, United States
D-U-N-S® Number: 87-422-6244
Has Not Opted Out of Direct Marketing

(S) Fiserv Spa
Nueve Providencia 2353, Providencia, Santiago, Chile
D-U-N-S® Number: 95-336-2775
Has Not Opted Out of Direct Marketing

(S) Chase Credit Systems, Inc
300 E Magnolia Blvd Ste 502, Burbank, California, 91502-1178, United States
D-U-N-S® Number: 87-453-9695
Has Not Opted Out of Direct Marketing

(S) Fiserv Investment Solutions, Inc.
255 Fiserv Dr, Brookfield, Wisconsin, 53045-5817, United States
D-U-N-S® Number: 01-341-4832
Has Not Opted Out of Direct Marketing

(S) Adviceamerica, Inc.
121 Mission Falls Ln, Fremont, California, 94539-7824, United States
D-U-N-S® Number: 11-200-8136
Has Not Opted Out of Direct Marketing

(HQ) Fiserv Solutions, LLC
255 Fiserv Dr, Brookfield, Wisconsin, 53045-5817, United States
D-U-N-S® Number: 08-926-9476
Has Not Opted Out of Direct Marketing

(S) Fiserv West Des Moines Center Inc
4400 Westown Pkwy Ste 400, West Des Moines, Iowa, 50266-6756, United States
D-U-N-S® Number: 09-311-0369
Has Not Opted Out of Direct Marketing

(HQ) Fiserv Cir Inc.
255 Fiserv Dr, Brookfield, Wisconsin, 53045-5817, United States
D-U-N-S® Number: 05-707-3744
Has Not Opted Out of Direct Marketing

(HQ) Fiserv UK Holding Ltd.
Eversheds House, Manchester, M1 5ES, United Kingdom
D-U-N-S® Number: 22-047-1537
Has Not Opted Out of Direct Marketing

(HQ) Fiserv Worldwide Holdings Ltd.
Eversheds House, Manchester, M1 5ES, United Kingdom
D-U-N-S® Number: 22-047-3376
Has Not Opted Out of Direct Marketing

(HQ) Checkfree Solutions Ltd.
1St Floor, Slough, SL1 1FQ, United Kingdom
D-U-N-S® Number: 77-121-8351
Has Not Opted Out of Direct Marketing

(HQ) Fiserv (Europe) Ltd.
7 Roundwood Avenue, Uxbridge, UB11 1AS, United Kingdom
D-U-N-S® Number: 50-499-2959
Has Not Opted Out of Direct Marketing

HQ FISERV (APAC) PTE. LTD.
12 Marina Boulevard, Singapore, 018982, Singapore
D-U-N-S® Number: 59-528-9729
Has Not Opted Out of Direct Marketing

S FISERV AUSTRALIA PTY LIMITED
L13 90 Arthur St, North Sydney, New South Wales, 2060, Australia
D-U-N-S® Number: 75-504-2942
Has Not Opted Out of Direct Marketing

HQ Information Technology, Inc.
1345 Old Cheney Rd, Lincoln, Nebraska, 68512-1266, United States
D-U-N-S® Number: 08-956-3498
Has Not Opted Out of Direct Marketing

HQ Precision Computer Systems, Inc.
4501 S Technology Dr, Sioux Falls, South Dakota, 57106-4213, United States
D-U-N-S® Number: 10-760-7590
Has Not Opted Out of Direct Marketing

HQ Xp Systems Corporation
405 Science Dr, Moorpark, California, 93021-2247, United States
D-U-N-S® Number: 78-136-8196
Has Not Opted Out of Direct Marketing

HQ I Tech Corporation.
4400 Westown Pkwy Ste 400, West Des Moines, Iowa, 50266-6756, United States
D-U-N-S® Number: 01-020-9158
Has Not Opted Out of Direct Marketing

HQ Open Solutions, LLC
455 Winding Brook Dr, Glastonbury, Connecticut, 06033-4315, United States
D-U-N-S® Number: 80-267-8524
Has Not Opted Out of Direct Marketing

HQ OPEN SOLUTIONS SOFTWARE SERVICES PRIVATE LIMITED
1St Floor,, Gurgaon, Haryana, 122002, India
D-U-N-S® Number: 91-583-0127
Has Not Opted Out of Direct Marketing

S The Weiland Financial Group Inc
2333 Waukegan Rd Ste 175, Bannockburn, Illinois, 60015-1541, United States
D-U-N-S® Number: 06-457-0344
Has Not Opted Out of Direct Marketing

S Precision Direct, Inc
19615 Russell Rd, Kent, Washington, 98032-1115, United States
D-U-N-S® Number: 17-549-0325
Has Not Opted Out of Direct Marketing

(HQ) Checkfree Services Corporation
2900 Westside Pkwy, Alpharetta, Georgia, 30004-7429, United States
D-U-N-S® Number: 14-721-2724
Has Not Opted Out of Direct Marketing

(S) Checkfree Services Corporation
255 Fiserv Dr, Brookfield, Wisconsin, 53045-5815, United States
D-U-N-S® Number: 06-348-1601
Has Not Opted Out of Direct Marketing

(HQ) Summit Information Systems Corporation
4500 Sw Research Way, Corvallis, Oregon, 97333-1093, United States
D-U-N-S® Number: 03-921-9399
Has Not Opted Out of Direct Marketing

(HQ) DOVETAIL GROUP LIMITED
Suite 3 One Earlsfort Terrace, Dublin, Ireland
D-U-N-S® Number: 98-536-8377
Has Not Opted Out of Direct Marketing

(HQ) DOVETAIL GROUP SERVICES LIMITED
Suite 3 One Earlsfort Centre, Dublin, 2, Ireland
D-U-N-S® Number: 98-552-8359
Has Not Opted Out of Direct Marketing

(S) DOVETAIL GROUP SERVICES LIMITED
Galleria Pattari 2, Milano, Milano, 20122, Italy
D-U-N-S® Number: 43-398-3412
Has Not Opted Out of Direct Marketing

(S) Dovetail Systems Ltd.
Dovetail Systems Limited, London, EC2V 7DA, United Kingdom
D-U-N-S® Number: 77-974-1524
Has Not Opted Out of Direct Marketing

(S) Fiserv Solutions, Inc.
575 Brick Church Park Dr, Nashville, Tennessee, 37207-3219, United States
D-U-N-S® Number: 10-206-9556
Has Not Opted Out of Direct Marketing

(HQ) Users Incorporated
1250 Drummers Ln, Valley Forge, Pennsylvania, 19482, United States
D-U-N-S® Number: 05-923-5031
Has Not Opted Out of Direct Marketing

(HQ) Fiserv Csw, Inc
125 Cambridgepark Dr Ste 2, Cambridge, Massachusetts, 02140-2329, United States
D-U-N-S® Number: 80-867-2935
Has Not Opted Out of Direct Marketing

(S) Epsiia Corporation
901 S Mo Pac Expy Ste Iii500, Austin, Texas, 78746-5918, United States
D-U-N-S® Number: 12-151-1232
Has Not Opted Out of Direct Marketing

(HQ) Cashedge Inc.
255 Fiserv Dr, Brookfield, Wisconsin, 53045-5815, United States
D-U-N-S® Number: 12-849-8495
Has Not Opted Out of Direct Marketing

(S) ITI of Nebraska Inc
1345 Old Cheney Rd, Lincoln, Nebraska, 68512-1266, United States
D-U-N-S® Number: 07-212-5375
Has Not Opted Out of Direct Marketing

(S) Billmatrix Corporation
8750 N Central Expy Ste 2000, Dallas, Texas, 75231-6433, United States
D-U-N-S® Number: 87-743-9448
Has Not Opted Out of Direct Marketing

(S) Dovetails Group Ltd.
5-6 George Street, St Albans, AL3 4ER, United Kingdom
D-U-N-S® Number: 22-078-6561
Has Not Opted Out of Direct Marketing

BACK TO TABLE OF CONTENTS

Corporate Overview

Location
255 Fiserv Dr
Brookfield, WI, 53045-5817
Waukesha County
United States

Tel: 262-879-5000

Marketability: Has Not Opted Out of Direct Marketing

www.fiserv.com

Quote Symbol - Exchange	FISV - NASDAQ
Sales USD(mil):	5,823.0
Assets USD(mil):	11,676.0
Employees:	24,000
Fiscal Year End:	31-Dec-2018
KeyID[SM]:	12138
Industry:	Computer Services

Incorporation Date:	198·
Company Type:	Public Parent
Quoted Status:	Quoted
President, CEO and Director:	Jeffery W. Yabuki

Key Corporate Relationships

Auditor: Deloitte & Touche LLP

Bank: Banc Of America Leasing & Capital Llc, Hewlett-Packard Financial Services, Ibm Credit Llc, Pnc Equipment Finance Llc, Suntrust Equipment Finance & Leasing Corp, Chase Equipment Leasing Inc

Industry Codes

NAICS 2017:

518210 - Data Processing, Hosting, and Related Services (Primary)
541511 - Custom Computer Programming Services

ISIC Rev 4:

6311 - Data processing, hosting and related activities (Primary)
6202 - Computer consultancy and computer facilities management activities

NACE 2002:

6311 - Data processing, hosting and related activities (Primary)
6202 - Computer consultancy activities

UK SIC 2007:

6311 - Data processing, hosting and related activities (Primary)
6202 - Computer consultancy activities

ANZSIC 2006:

7000 - Computer System Design and Related Services (Primary)

UK SIC 2003:

7230 - Data processing (Primary)
7222 - Other software consultancy and supply

US SIC 1987:

7374 - Computer Processing and Data Preparation and Processing Services (Primary)
7371 - Computer Programming Services

US 8-Digit SIC:

73749902 - Data processing service (Primary)
73710300 - Computer software development and applications

Business Description

Fiserv Inc. provides financial companies with the technology services they need to operate. The company provides core processing systems, electronic billing and payment systems, ATM management, and loan processing services to banks, thrifts, credit unions, and other financial institutions. It also provides licensed software, consulting, and other support services. Fiserv serves customers of all sizes, but its bread and butter has traditionally been small to midsized banks without in-house processing units. Other clients include insurance companies, merchants, leasing firms, and government agencies. Fiserv agreed to buy First Data, a payments processor, for $22 billion.

Source: D&B

More Business Descriptions

Fiserv Inc (Fiserv) is a provider of financial services technology. The company provides internet and mobile banking systems, account processing systems, electronic payments processing products and services. It also offers services including document and payment card production and distribution, check processing and imaging, source capture systems, and lending and risk management products and services. It serves to a wide range of markets including banks, savings banks, government, insurance, healthcare, telecommunications, utilities, wealth management, De Novo, retail and commerce, credit unions, investment management firms, leasing and finance companies, billers, merchants, associations, and building societies. Fiserv is headquartered in Brookfield, Wisconsin, the US.The company reported revenues of (US Dollars) US$5,823 million for the fiscal year ended December 2018 (FY2018), an increase of 2.2% over FY2017. In FY2018, the company's operating margin was 29.9%, compared to an operating margin of 26.9% in FY2017. In FY2018, the company recorded a net margin of 20.4%, compared to a net margin of 21.9% in FY2017.The company reported revenues of US$1,502.0 million for the first quarter ended March 2019, a decrease of 3.2% over the previous quarter.

Source: Global Data

Fiserv Inc (Fiserv) is a provider of financial services technology. The company provides electronic payments processing products and services, account processing systems, internet and mobile banking systems and other related services. The company classifies its business operations into two reportable segments: Payments and Industry Products (Payments) and Financial Institution Services (Financial). Fiserv serves to more than 12,000 clients worldwide, including banks, credit unions, leasing and finance companies, investment management firms, retailers, merchants and government agencies.

Source: Global Data

Financial Data

Financials in:	USD(mil)	1 Year Growth
Revenue:	5,823.0	2.2%
Assets:	11,676.0	9.5%
Date of Financial Data:	31-Dec-2018	

Market Data

Quote Symbol:	FISV
Exchange:	NASDAQ
Currency:	USD
Stock Price:	94.5
Stock Price Date:	07-12-2019
Market Value (mil):	37,089.5

Additional Information

Fortune 1000 Rank:	488

© 2019 Dun & Bradstreet, Inc. All rights reserved. © 2019 Morningstar. All Rights Reserved. © 2019 GlobalData. All Rights Reserved.

BACK TO TABLE OF CONTENTS

Signals Report

100 Does Business in UK

The value of this signal is set to 100 when a company does business in UK, zero otherwise. Determined for all possible companies in the D&B Hoovers database. Updated at least quarterly.

100 Does Business in India

The value of this signal is set to 100 when a company does business in India, zero otherwise. Determined for all possible companies in the D&B Hoovers database. Updated at least quarterly.

100 Does Business in United States

The value of this signal is set to 100 when a company does business in the United States, zero otherwise. Determined for all possible companies in the D&B Hoovers database. Updated at least quarterly.

100 Mobile Enabled

Signals when a company has corporate web site that supports mobile access or has applications developed for mobile devices.

100 Minority Friendly

Signals the likelihood that the company has minority-friendly workplace and policies based on evidence found in news stories, the company website, and other information sources.

100 Technology Adopter

Signals the likelihood that a company is a strong adopter of technology solutions based on evidence found in news stories, the company website, and other information sources.

99 Recent News Presence

Signals the level of a company's business news presence relative to other companies with news presence over the last 90 days.

99 Importer

Signals the likelihood that a company is an importer based on evidence found in news stories, the company website, and other information sources.

98 Divesting Activity

A signal value of 1-100 reflects the degree to which a company is referenced in press releases, business press articles, or SEC filings that discuss the divestiture of businesses or assets. 0 indicates that no activity was detected. Measures activity detected over the past 90 days.

98 Recent Press Release Presence

Signals the level of a company's press release presence relative to other companies who distributed press releases over the last 90 days.

97 M&A Activity

Scores a company's merger and acquisition activity based on press releases, business press articles, or SEC filings. The value is a percentile ranking within all companies in the D&B Hoovers database for the same activity. 0 means no activity was detected. All companies in the D&B Hoovers Database where any activity was detected. Measures activity detected over the past 90 days.

97 SAP ERP

Signals the likelihood that a company utilizes SAP ERP software or technology based on information found in news stories, the company's website, and other sources.

95 Symantec

Signals the likelihood that a company utilizes Symantec software or technology based on information found in news stories, the company's website, and other sources.

82 Going Public Activity

Scores a company's initial public offering activity based on press releases, business press articles, or SEC filings. The value is a percentile ranking within all companies in the D&B Hoovers database for the same activity. 0 means no activity was detected. All companies in the D&B Hoovers Database where the same activity was detected. Measures activity detected over the past 90 days.

79 Conference Participation

A signal value of 1-100 reflects the degree to which a company is referenced in press releases, business press articles, or SEC filings that discuss conference participation. 0 indicates that no activity was detected. Measures activity detected over the past 90 days.

78 Venture Financing Activity

Scores a company's venture financing activity based on press releases, business press articles, or SEC filings. The value is a percentile ranking within all companies in the D&B Hoovers database for the same activity. 0 means no activity was detected. All companies in the D&B Hoovers Database where any activity was detected. Measures activity detected over the past 90 days.

77 Big Data

Signals the likelihood that a company provides products or services related to the storage or analysis of big data based on information found in news stories, the company's website, and other sources.

68 High Bandwidth

Signals the likelihood that a company requires high communication bandwidth based on its aggregate ranking for other relevant signals.

67 Ecommerce

Signals the extent to which a company in the D&B Hoovers database utilizes Ecommerce as a sales channel or transaction platform or delivers software or services that enable Ecommerce.

64 Product Launches

Scores a company's product launch activity based on press releases, business press articles, or SEC filings. The value is a percentile ranking of a company's level of news, filing, and PR activity regarding a Product Launch across all companies in the D&B Hoovers Database where activity was detected. Measures activity detected over the past 90 days.

64 Salesforce.com

Signals the likelihood that a company utilizes Salesforce.com software or technology based on information found in news stories, the company's website, and other sources.

55 Relocation Activity

Scores a company's relocation activity based on press releases, business press articles, or SEC filings. The value is a percentile ranking of a company's level of news, filing, and PR activity regarding Relocation across all companies in the D&B Hoovers Database where activity was detected. Measures activity detected over the past 90 days.

54 PeopleSoft

Signals the likelihood that a company utilizes PeopleSoft software or technology based on information found in news stories, the company's website, and other sources.

30 Social Media Presence

Signals the extent to which a company promotes Social Media channels for communications on its corporate web site for all companies in the D&B Hoovers database where a corporate URL is available.

29 Legal Issues

Scores a company's legal activity based on press releases, business press articles, or SEC filings. The value is a percentile ranking of a company's level of news, filing, and PR activity regarding Legal Issues across all companies in the D&B Hoovers Database where activity was detected. Measures activity detected over the past 90 days.

22 Services are Cloud Hosted

Signals the likelihood that a company provides cloud-hosted products and services based on information found in news stories, the company's website, and other sources.

15 Female Friendly

Signals the likelihood that the company has woman-friendly workplace and policies based on evidence found in news stories, the company website, and other information sources.

2 All Executive Change Activity

The value is a percentile ranking of a company's level of news, filing, and PR activity regarding All executive changes across all companies in the D&B Hoovers Database where activity was detected. Measures activity detected over the past 90 days.

SWOT Analysis

	Positive	Negative
Internal Organizational Attributes	**Strengths** • Customer Base • Operational Performance • End Markets	**Weaknesses** • Substantial Debt
External Environmental Attributes	**Opportunities** • Payment Channels Market in the US • Launch of New Products • Contracts	**Threats** • Foreign Exchange Risks • Government Regulations • Intense Competition

Overview

Fiserv Inc (Fiserv) is a provider of technology solutions to banks, credit unions, financial planners and investment advisers. Customer base, operational performance, end markets are the company's major strengths, whereas substantial debt remains causes for concern. Payment channels market in the US, launch of new products, contracts are likely to offer growth opportunities to the company. However, intense competition, foreign exchange risks, government regulations could affect its business opportunities.

Strengths

Customer Base

Strong customer base builds strong brand equity for the company and helps it to streamline its business operations. The company has more than 12,000 clients and 24,000 associates worldwide. Finserv offers its services to banks, credit unions, financial planners and investment advisers, insurance companies and agents, leasing companies, lenders, savings institutions, retailers and merchants, government bodies, and publicly and privately owned companies. The company provides technology platforms and software solutions to about 300 financial firms including broker dealers, global asset managers, investment advisors, banks and insurance companies. As of December 31 2018, over 2,500 clients financial institutions agreed to provide Fiserv's person-to-person payments services to their customers. Also in the same period, the company had over 2,300 Mobiliti ASP clients utilizing Finserv's digital channel services.

Operational Performance

The company's operational performance increased during the review year. Operating margin of the company stood at 29.8% for the last fiscal year and outperformed the Cards & Payments industry operating margin average of 7.9% for the same year. The strong operating margin of the company can be attributed to an optimal pricing strategy and operational efficiency. It also showcases company's ability to create value for shareholders with positive operating cash and fulfill obligations towards the creditors. Its operating cost as a percentage of sales declined from 73.1% in FY2017 to 70.1% in FY2018. The company's return on equity (ROE) stood at 51.7% for the last fiscal year, which was higher than the Cards & Payments industry average ROE of 7.3% for the same year. The strong ROE shows that the company is efficient in utilizing its equity base in delivering better results to its shareholders.

End Markets

The company's presence in a wide range of end markets helps it in mitigating risks associated with dependence on a select market. Finserv serves wide range of industries like associations, banks, credit unions, billers, business banking, government institutions, lending, thrifts, wealth management, property management, utilities, healthcare, property management, corporate services, insurance, institutional asset management, telecommunications, retail and commerce, and De Novo financial institutions. The company also undertakes and executes various partnership programs, which serve a large customer base in the domestic and international markets. Such a diversified markets served by the company will help in increasing the revenues, whilst positively affecting the company's long term prospects.

Weaknesses

Substantial Debt

Fiserv has substantial debts, which may adversely affect its operations. The company reported total debt of US$5959 million during FY2018, a year-on-year increase of 21.6%. The significant increase in debt limits its ability to obtain additional financing in future for working capital, and for other strategic initiatives. Substantial debts may adversely affect the company's operations and may further weaken its financial position.

Opportunities

Payment Channels Market in the US

The growing market for payment channels in the US could provide growth opportunities to the company. According to in-house report, the number of cards in circulation in the country is projected to reach 1,653.1 million in 2022, with 921.2 million debit cards, 708.4 million credit cards, and 23.6 million charge cards. The transaction value of the channels is forecast to grow to US$9,172.8 billion in 2022, including US$4,266.8 billion for debit cards, US$4,578.9 billion for credit cards, and US$327.1 billion for charge cards. The growth could be the result of increasing mobile payments, growth in e-commerce, increase in the number of contactless terminals, and migration to Europay, MasterCard and Visa standards.

Launch of New Products

The company focuses on the expansion of its product portfolio through the launch of new products. In February 2019, Fiserv announced a new Mortgage Momentum a digital-focused approach that allows lenders to manage the complex mortgage ecosystem from end-to-end. In September 2018, the company launched Originate, a new suite of the solution, for the challenges faced by the Online account opening and Loan applications. Originate helps credit unions and banks to deliver digital account opening and loan origination. In August 2018, the company introduced two enhanced consumer authentication solutions, step-up authentication and identity verification to mitigate card fraud within call centers. In April 2018, the company launched FinKit, for assisting financial institutions and meet rapidly unfolding regulations. The kit is developed to enable long-term compliance and capabilities to increase the open banking opportunities.

Contracts

The firm's reputation in the market makes it preferred advisor for several large organization in the financial services industry. It clients base includes banks, thrifts, credit unions, investment management firms, leasing and finance companies, retailers, and merchants located globally. In June 2018, the company entered into a partnership with VyStar Credit Union (VyStar), to improve mobile banking app with innovative card control features of VyStar. In April 2018, the company announced a strategic partnership with Farmers & Merchants Savings Bank, to drive growth with an enhanced customer experience of Farmers & Merchants Savings Bank. In February 2018, Kawartha Credit Union selected Fiserv to streamline operations and enhance the credit union's ability to deliver highly personalized services. In January 2018, the company partnered with Motor City Community Credit Union to leverage the technology and flexibility of the DNA account processing platform. In the same month, Fiserv expanded its partnership with First Foundation Bank, to meet the growing technological needs of First Foundation Bank's diverse customer base.

Threat

Foreign Exchange Risks

The company operates in many parts of the world and it is exposed to fluctuations in foreign exchange rates. The company reports financials in the US Dollar and as a result, its revenue is exposed to volatility of the US Dollar against other functional currencies, as it serves customers across the world. The major elements exposed to exchange rate risks include the company's investments in overseas subsidiaries and affiliates and monetary assets and liabilities arising from business transactions in foreign currencies. In FY2018, the company reported a loss of US$13 million from foreign currency translation adjustments. To minimize risks from currency fluctuations, the company could involve in foreign exchange hedging activities by entering into foreign exchange forward contracts. However, there could be no assurance that such hedging or measures would limit the impact of movements in exchange rates on the company's results of operations.

Government Regulations

The company's operations always subject to strict regulations of different regulators and federal agencies. The company provides primarily its services to financial institutions and intermediaries. Due to direct business involvement with financial institutions and intermediaries, the companies processing and electronic commerce are examined on a regular basis by the Federal Deposit Insurance Corporation (FDIC), the Federal Reserve Bank, National Credit Union Association, Office of Thrift Supervision, Office of the Comptroller of the Currency and various state regulatory authorities. The company is also subject to Federal Reserve Board's rules with respect to its ACH network. Further, other operations of Fiserv are also subject to different rules and regulations across the world related to procession and transaction service platforms. In light of any sudden change in any of the rules and regulations, the company's business operations will be adversely affected.

Intense Competition

The company operates in a highly competitive financial services market. The factors that determine the level of competition within the industry include service performance, price, and sales and distribution capabilities. Finserv faces competition from Fidelity National Information Services, Inc. (Fidelity National), Heartland Payment Systems, Inc. (Heartland Payment) and Global Payments Inc. (Global Payments) Apart from established players in developed countries, players from emerging countries are also competing hard to garner greater market share. Many of its competitors have a longer operating history, greater brand recognition, established customer and supplier relationships, and greater financial resources, which leads to the creation of innovative products and business expansion through acquisitions. In March 2019, Global Payments acquired Sentral Education, a provider of cloud-based school administration software solutions. The acquisition enables the company to enables the company to design products utilizing cloud based solutions., to cater customer needs. In November 2018, Fidelity National partnered with LVMH Group (LVMH) to connect LVMH with SWIFT Global Payments Innovation. The partnership will allow LVMH to speed up its cross-border payments. The initiative could also enhance the company's revenue by selling its services to LVMH.

Copyright © 2019 GlobalData. All Rights Reserved.
Published by Dun & Bradstreet, Inc., July, 2019

BACK TO TABLE OF CONTENTS

News

Tech Know Bits
23-Jul-2019 (663 words)

Fiserv (FISV) Set to Announce Earnings on Thursday

Fiserv (NASDAQ:FISV) is set to post its quarterly earnings results after the market closes on Thursday, July 25th. Analysts expect Fiserv to post earnings of $0.80 per share for the quarter. Fiserv has set its FY 2019 guidance at $3.39-3.52 EPS and its FY19 guidance at $3.39-3.52 EPS. Fiserv (NASDAQ:FISV) last announced its earnings results on Tuesday, April 30th. The business...
www.techknowbits.com

PYMNTS
22-Jul-2019 (112 words)

PYMNTS.com

The monthly Faster Payments Tracker, powered by Fiserv, is your go-to resource for staying up to date on faster payments...
www.pymnts.com

Newsroom
22-Jul-2019 (519 words)

Survey of Mexico Residents Shows Banking Interactions Impact Daily Life

BROOKFIELD, Wis. & MEXICO CITY, July 22, 2019 – Customer expectations are advancing faster than ever. Fortunately, new technologies and a growing preference for digital interactions can help financial institutions meet these expectations. Technology can help financial institutions operate more efficiently, differentiate from competitors and better serve customers by streamlining...
www.newsroom.fiserv.com

Milwaukee Journal Sentinel
18-Jul-2019 (498 words)

Service and hospitality unionizers demand better workplace conditions from Fiserv Forum contractors

Members and supporters of the Milwaukee Area Service and Hospitality Workers Organization rallied Thursday on the Deer District Plaza before entering initial negotiations for with Fiserv Forum contractors for higher wages. The union, referred to as MASH, met with Levy Premium Foodservice for three hours to hash out initial grounds for a contract improving workplace conditions for the...
www.jsonline.com

Futures Trading Charts
18-Jul-2019 (225 words)

Fiserv Inc Rises 1.52% on Heavy Volume: Watch For Potential Pullback

Jul 18, 2019 (SmarTrend(R) News Watch via COMTEX) -- Fiserv Inc (NASDAQ:FISV) traded in a range yesterday that spanned from a low of $93.43 to a high of $95.71. Yesterday, the shares gained 1.5%,...
www.futures.tradingcharts.com

U.S. Securities and Exchange Commission
18-Jul-2019 (644 words)

FISERV INC; YABUKI JEFFERY W; Form 4 Insider Buying and Selling; 2019-07-17

SEC FORM 4 SEC Form 4 FORM 4 UNITED STATES SECURITIES AND EXCHANGE COMMISSION Washington, D.C. 20549 STATEMENT OF CHANGES IN BENEFICIAL OWNERSHIP Filed pursuant to Section 16(a) of the Securities Exchange Act of 1934 or Section 30(h) of the Investment Company Act of 1940 OMB APPROVAL OMB Number: 3235-0287 Estimated average burden hours per response: 0.5 Check this box if no long...
www.sec.gov

MR Modern Readers
18-Jul-2019 (842 words)

Q2 2019 EPS Estimates for Fiserv Inc Reduced by Wedbush (NASDAQ:FISV)

Fiserv Inc (NASDAQ:FISV) – Research analysts at Wedbush decreased their Q2 2019 earnings estimates for shares of Fiserv in a research report issued on Monday, July 15th. Wedbush analyst M. Katri now anticipates that the business services provider will earn $0.81 per share for the quarter, down from their previous forecast of $0.83. Wedbush has a "Outperform" rating and a $105.00 price...
www.modernreaders.com

WSB News.Talk Radio
17-Jul-2019 (285 words)

BREAKING: 2 employees detained during sweep of Fiserv building in Alpharetta

Two employees were detained during an active shooter scare that prompted the evacuation of an Alpharetta business Tuesday, according to Channel 2 Action News. An incident report obtained Wednesday by the news station indicates the workers were detained...
www.wsbradio.com

U.S. Securities and Exchange Commission
17-Jul-2019 (1,223 words)

FIRST DATA CORP: 8-K - Other Events

8-K 1 d777787d8k.htm 8-K 8-K UNITED STATES SECURITIES AND EXCHANGE COMMISSION Washington, D.C. 20549 FORM 8-K CURRENT REPORT Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 Date of Report (Date of earliest event reported): July 17, 2019 First Data Corporation (Exact Name of Registrant as Specified in Charter) Delaware 001-11073 47-0731996 (State or Other Jurisdiction of I...
www.sec.gov

U.S. Securities and Exchange Commission
17-Jul-2019 (1,213 words)

FISERV INC: 8-K - Other Events

8-K 1 d777816d8k.htm 8-K 8-K UNITED STATES SECURITIES AND EXCHANGE COMMISSION Washington, D.C. 20549 FORM 8-K CURRENT REPORT PURSUANT TO SECTION 13 OR 15(D) OF THE SECURITIES EXCHANGE ACT OF 1934 Date of Report (Date of earliest event reported): July 17, 2019 Fiserv, Inc. (Exact Name of Registrant as Specified in Its Charter) Wisconsin 1-38962 39-1506125 (State or Other Jurisdiction of Incorpor...
www.sec.gov

BACK TO TABLE OF CONTENTS

Triggers

NEWS: DIVESTITURES (5 days ago)
18-Jul-2019 07:28 GMT

Q2 2019 EPS Estimates for Fiserv Inc Reduced by Wedbush (NASDAQ:FISV)

Jeffery W. Yabuki **sold 20,000 shares** of the firm's stock in a transaction on Wednesday, May 15th. The stock was sold at an average price of $85.49, for a total transaction of $1,709,800.00. The transaction was disclosed in a document filed with the Securities & Exchange Commission, which is available through this link . Also, insider Jeffery W. Yabuki **sold 2,000 shares** of the firm's stock in a transaction on Tuesday, May 21st. The stock was sold at an average price of $88.
Companies in Event: Fiserv, Inc.,
Related Contacts: Jeffery Yabuki,

NEWS: CLOSING FACILITIES (6 days ago)
17-Jul-2019 11:00 GMT

FIRST DATA CORP: 8-K - Other Events

Securities and Exchange Commission (the ?SEC?) and those identified elsewhere in this communication, the following factors, among others, could cause actual results to differ materially from forward-looking statements or historical performance: the occurrence of any event, change or other circumstances that could give rise to the right of one or both of First Data and Fiserv to terminate the definitive merger agreement between First Data and Fiserv; the outcome of any legal proceedings ...
Companies in Event: Fiserv, Inc.,

NEWS: EARNINGS RESULTS (7 days ago)
16-Jul-2019 13:38 GMT

Fiserv (NASDAQ:FISV) Given New $105.00 Price Target at Wedbush

During the same quarter in the prior year, the firm posted $0.76 earnings per share. As a group, research analysts forecast that Fiserv will post 3.44 EPS for the current fiscal year. In related news, insider Jeffery W. Yabuki sold 2,000 shares of the company's stock in a transaction dated Tuesday, May 21st. The shares were sold at an average price of $88.95, for a total value of $177,900.00. Following the sale, the insider now owns 371,429 shares in the company, valued at approximately ...
Companies in Event: Fiserv, Inc.,
Related Contacts: Jeffery Yabuki,

NEWS: EARNINGS ANNOUNCEMENT (8 days ago)
15-Jul-2019 21:58 GMT

Fiserv to Release Second Quarter Earnings Results on July 25, 2019

BROOKFIELD, Wis.--(BUSINESS WIRE)--Jul. 15, 2019-- **Fiserv**, Inc. (**NASDAQ: FISV**), a leading global provider of financial services technology solutions, will **announce its second quarter financial results after the** close of regular market trading on Tuesday, July 25, 2019. The company will discuss the results in a live webcast at 4 p.m. CT. The webcast, along with supplemental financial information, can be accessed on the investor relations section of the **Fiserv** website at investors.
Companies in Event: Fiserv, Inc.,

NEWS: MERGERS AND ACQUISITIONS (11 days ago)
12-Jul-2019 11:57 GMT

CMA Investigates And Clears Fiserv Merger With First Data - Quick Facts

The Competition and Markets Authority announced Friday that it has decided not to refer the anticipated acquisition by Fiserv Inc. (FISV) of First Data Corp. (FDC) to Phase II. It has investigated and cleared the proposed acquisition. Fiserv agreed in mid-January to acquire First Data in an all-stock transaction valued at $22 billion. Following the close of the all-stock transaction, Fiserv shareholders will own 57.
Companies in Event: Fiserv, Inc., First Data Corp.

NEWS: STOCK TRADES (17 days ago)
6-Jul-2019 08:17 GMT

Jeffery W. Yabuki Sells 20,000 Shares of Fiserv Inc (NASDAQ:FISV) Stock

Fiserv Inc (**NASDAQ:FISV**) insider Jeffery W. Yabuki **sold 20,000 shares** of the company's stock in a transaction that occurred on Wednesday, June 19th. The stock was sold at an average price of $89.23, for a total transaction of $1,784,600.00. Following the transaction, the insider now owns 354,929 shares in the company, valued at $31,670,314.
Companies in Event: Fiserv, Inc.,
Related Contacts: Jeffery Yabuki,

NEWS: DIVESTITURES (17 days ago)
6-Jul-2019 08:17 GMT

Jeffery W. Yabuki Sells 20,000 Shares of Fiserv Inc (NASDAQ:FISV) Stock

Fiserv Inc (**NASDAQ:FISV**) insider Jeffery W. Yabuki **sold 20,000 shares** of the company's stock in a transaction that occurred on Wednesday, June 19th. The stock was sold at an average price of $89.23, for a total transaction of $1,784,600.00. Following the transaction, the insider now owns 354,929 shares in the company, valued at $31,670,314.67. The sale was disclosed in a filing with the Securities & Exchange Commission, which is available at this link . Jeffery W.
Companies in Event: Fiserv, Inc.,
Related Contacts: Jeffery Yabuki,

NEWS: DIVESTITURES (17 days ago)
6-Jul-2019 04:32 GMT

Tyers Asset Management LLC Acquires 1,316 Shares of Fiserv Inc (NASDAQ:FISV)

The firm owned 25,256 shares of the business services provider's stock after purchasing an additional 1,316 shares during the quarter. Tyers Asset Management LLC's holdings in **Fiserv** were worth $2,230,000 as of its most recent SEC filing. Other large investors have also bought **and sold shares** of the company. Lazard Asset Management LLC grew its stake in **Fiserv** by 857.8% during the 1st quarter. Lazard Asset Management LLC now owns 3,493,843 shares of the business services provider's stock worth $308,435,000 after purchasing an additional 3,129,050
Companies in Event: Fiserv, Inc.,
Related Contacts: Jeffery Yabuki,

NEWS: EARNINGS RESULTS (18 days ago)
6-Jul-2019 02:32 GMT

Fiserv (NASDAQ:FISV) Price Target Raised to $105.00 at Oppenheimer

PEG ratio of 2.28 and a beta of 0.78. **Fiserv** has a fifty-two week low of $68.45 and a fifty-two week high of $94.48. The company has a debt-to-equity ratio of 2.45, a quick ratio of 1.07 and a current ratio of 1.07. **Fiserv** (**NASDAQ:FISV**) last **announced its earnings results on Tuesday**, April 30th. The business services provider reported $0.84 EPS for the quarter, beating analysts' consensus estimates of $0.82 by $0.02. The business had revenue of $1.50 billion for the quarter, compared to analysts' expectations of $1.51 billion. **Fiserv** had a net
Companies in Event: Fiserv, Inc.,
Related Contacts: Jeffery Yabuki,

NEWS: DIVESTITURES (a month ago)
27-Jun-2019 10:27 GMT

Clarius Group LLC Takes Position in Fiserv Inc (NASDAQ:FISV)

On average, equities research analysts anticipate that **Fiserv** Inc will **post 3.45 earnings per share** for the current year. In other **Fiserv** news, insider Jeffery W. Yabuki **sold 2,000 shares** of **Fiserv** stock in a transaction on Tuesday, May 21st. **The shares were sold** at an average price of $88.95, for a total transaction of $177,900.00. Following the completion of the sale, the insider now owns 371,429 shares of the company's stock, valued at approximately $33,038,609.55. The transaction was disclosed in a document filed with the Securities & Exchange Commission,
Companies in Event: Fiserv, Inc.,
Related Contacts: Jeffery Yabuki,

BACK TO TABLE OF CONTENTS

Competitors

ACCENTURE PUBLIC LIMITED COMPANY
1 Grand Canal Square, Dublin, 2, Ireland
D-U-N-S® Number: 98-501-5354
Has Not Opted Out of Direct Marketing

Aci Worldwide, Inc.
3520 Kraft Rd Ste 300, Naples, Florida, 34105-4957, United States
D-U-N-S® Number: 84-748-6990
Has Not Opted Out of Direct Marketing

Ba Merchant Services
1231 Durrett Ln, Louisville, Kentucky, 40213-2041, United States
D-U-N-S® Number: 11-595-9744
Has Not Opted Out of Direct Marketing

CGI Inc
1350 Boul René-Lévesque O Suite 25E, Montréal, Quebec, H3G 1T4, Canada
D-U-N-S® Number: 24-851-3116
Has Not Opted Out of Direct Marketing

Fidelity National Information Services, Inc.
601 Riverside Ave, Jacksonville, Florida, 32204-2957, United States
D-U-N-S® Number: 03-077-2334
Has Not Opted Out of Direct Marketing

Finastra USA Corporation
555 Sw Morrison St # 300, Portland, Oregon, 97204-1440, United States
D-U-N-S® Number: 09-129-3753
Has Not Opted Out of Direct Marketing

First Data Corporation
225 Liberty St Fl 29, New York, New York, 10281-1049, United States
D-U-N-S® Number: 60-436-0081
Has Not Opted Out of Direct Marketing

Fis Data Systems Inc.
200 Campus Dr, Collegeville, Pennsylvania, 19426-4903, United States
D-U-N-S® Number: 10-142-2731
Has Not Opted Out of Direct Marketing

Intuit Inc.
2700 Coast Ave, Mountain View, California, 94043-1140, United States
D-U-N-S® Number: 11-329-0969
Has Not Opted Out of Direct Marketing

Jack Henry & Associates, Inc.
663 W Highway 60, Monett, Missouri, 65708-8215, United States
D-U-N-S® Number: 09-826-5341
Has Not Opted Out of Direct Marketing

Mastercard Incorporated
2000 Purchase St, Purchase, New York, 10577-2509, United States
D-U-N-S® Number: 11-856-9339
Has Not Opted Out of Direct Marketing

NCR Corporation
864 Spring St Nw, Atlanta, Georgia, 30308-1007, United States
D-U-N-S® Number: 00-131-6090
Has Not Opted Out of Direct Marketing

Paypal Holdings, Inc.
2211 N 1st St, San Jose, California, 95131-2021, United States
D-U-N-S® Number: 07-980-9888
Has Not Opted Out of Direct Marketing

The Western Union Company
7001 E Belleview Ave, Denver, Colorado, 80237-2738, United States
D-U-N-S® Number: 78-780-8950
Has Not Opted Out of Direct Marketing

Total System Services, Inc.
1 Tsys Way, Columbus, Georgia, 31901-4222, United States
D-U-N-S® Number: 10-199-1222
Has Not Opted Out of Direct Marketing

Visa Inc.
900 Metro Center Blvd, Foster City, California, 94404-2775, United States
D-U-N-S® Number: 80-804-0260
Has Not Opted Out of Direct Marketing

Worldpay, Inc.
8500 Governors Hill Dr, Symmes Twp, Ohio, 45249-1384, United States
D-U-N-S® Number: 07-843-3177
Has Not Opted Out of Direct Marketing

© 2018 Dun & Bradstreet, Inc. All rights reserved. (Noted as D&B)

BACK TO TABLE OF CONTENTS

Closest Industry Peers

Checkfree Services Corporation

Data Processing

Brookfield, Wisconsin, United States
Sales USD: 793k , Employees: 9 (This Site) 9 (All Sites) , Type: Private Subsidiary,

Phone: 678-375-1286
Distance: 0 km

Fiserv Cir Inc.

Data Processing

Brookfield, Wisconsin, United States
Sales USD: 106M , Employees: 600 (This Site) 1.3k (All Sites) , Assets: 6B , Type: Private Subsidiary, Headquarters,

Phone: 262-879-5000
URL: http://www.fiserv.com
Distance: 0 km

Fiserv, Inc.

Data Processing

Brookfield, Wisconsin, United States
Employees: 30 (This Site) , Type: Private Branch,

Phone: 800-425-3478
URL: http://www.fiserv.com
Distance: 0 km

Fiserv Global Services, Inc.

Data Processing

Brookfield, Wisconsin, United States
Sales USD: 39k , Employees: 2 (This Site) 2 (All Sites) , Type: Private Subsidiary, Headquarters,

Phone: 262-879-5000
Distance: 0 km

Fiserv Investment Solutions, Inc.

Data Processing

Brookfield, Wisconsin, United States
Sales USD: 102k , Employees: 1 (This Site) 1 (All Sites) , Type: Private Subsidiary,

Phone: 262-879-5000
Distance: 0 km

Fiserv Solutions, LLC

Data Processing

Brookfield, Wisconsin, United States
Sales USD: 301M , Employees: 500 (This Site) 5.2k (All Sites) , Type: Private Subsidiary, Headquarters,

Phone: 262-879-5000
URL: http://www.fiserv.com
Distance: 0 km

Square 2 Marketing, Inc.

Data Processing

Brookfield, Wisconsin, United States
Employees: 1 (This Site) , Type: Private Branch,

Phone: 414-431-8615
URL: http://www.square2marketing.com
Distance: 1.18 km

Dan Dorszynski

Data Processing

Brookfield, Wisconsin, United States
Sales USD: 76k , Employees: 2 (This Site) 2 (All Sites) , Type: Partnership Independent,

Phone: 262-439-9712
Distance: 2.57 km

Fortress Data Services LLC

Data Processing

Brookfield, Wisconsin, United States
Sales USD: 52k , Employees: 1 (This Site) 1 (All Sites) , Type: Private Independent,

Phone: 262-751-2323
Distance: 3.93 km

Eis, Inc.

Data Processing

New Berlin, Wisconsin, United States
Employees: 12 (This Site) , Type: Private Branch,

Phone: 888-988-5546
Distance: 3.95 km

BACK TO TABLE OF CONTENTS

Closest Companies

Checkfree Services Corporation

Data Processing

Brookfield, Wisconsin, United States
Sales USD: 793k , Employees: 9 (This Site) 9 (All Sites) , Type: Private Subsidiary,

Phone: 678-375-1286
Distance: 0 km

Accel/Exchange

Nonclassifiable Establishments

Brookfield, Wisconsin, United States
Type: Private Independent,

Phone: 800-519-8883
URL: http://www.accelnetwork.com
Distance: 0 km

Fiserv Cir Inc.

Data Processing

Brookfield, Wisconsin, United States
Sales USD: 106M , Employees: 600 (This Site) 1.3k (All Sites) , Assets: 62 , Type: Private Subsidiary, Headquarters,

Phone: 262-879-5000
URL: http://www.fiserv.com
Distance: 0 km

Fiserv, Inc.

Data Processing

Brookfield, Wisconsin, United States
Employees: 30 (This Site) , Type: Private Branch,

Phone: 800-425-3478
URL: http://www.fiserv.com
Distance: 0 km

Fiserv Global Services, Inc.

Data Processing

Brookfield, Wisconsin, United States
Sales USD: 39k , Employees: 2 (This Site) 2 (All Sites) , Type: Private Subsidiary, Headquarters,

Phone: 262-879-5000
Distance: 0 km

Fiserv Investment Solutions, Inc.

Data Processing

Brookfield, Wisconsin, United States
Sales USD: 102k , Employees: 1 (This Site) 1 (All Sites) , Type: Private Subsidiary,

Phone: 262-879-5000
Distance: 0 km

Fiserv Solutions, LLC

Data Processing

Brookfield, Wisconsin, United States
Sales USD: 891M , Employees: 500 (This Site) 5.2k (All Sites) , Type: Private Subsidiary, Headquarters,

Phone: 262-879-5000
URL: http://www.fiserv.com
Distance: 0 km

Fiserv Federal Systems, Inc.

Consulting Services

Brookfield, Wisconsin, United States
Sales USD: 17M , Employees: 2 (This Site) 9 (All Sites) , Type: Private Subsidiary, Headquarters,

Phone: 262-879-5000
Distance: 0 km

Interpoynt, LLC

Miscellaneous Professional Services

Brookfield, Wisconsin, United States
Sales USD: 28k , Employees: 1 (This Site) 1 (All Sites) , Type: Private Independent,

Phone: 262-879-5000
URL: http://www.fiserv.com
Distance: 0 km

Antinori Software, Inc.

Software

Brookfield, Wisconsin, United States
Sales USD: 65k , Employees: 2 (This Site) 2 (All Sites) , Type: Private Independent,

Phone: 262-879-5000
Distance: 0 km

BACK TO TABLE OF CONTENTS

Analyst Reports

Analyst Report
15-Jul-2019 (8 Pages)

Raising PT To $105 on Accretion Potential; Model Tweak In Line With the Street

Wedbush Securities Inc.

Analyst Report
12-Jun-2019 (13 Pages)

Revisiting FIS and FISV Respective Merger Pro Forma(s); Raising Targets

Oppenheimer & Co., Inc.

Analyst Report
5-Jun-2019 (14 Pages)

Compelling Compounding. Raise To Buy.

SunTrust Robinson Humphrey Capital Markets

Analyst Report
6-May-2019 (9 Pages)

First Data Strength Boosts Outlook

The Buckingham Research Group

BACK TO TABLE OF CONTENTS

UCC Filings

171 Results

Filing Date	Filing No.	Filing Type	Secured Party	Collateral	Asset Type
2018/08/04	180010726521	Continuation	HEWLETT-PACKARD FINANCIAL SERVICES COMPANY		
2018/08/02	180010649626	Continuation	PNC EQUIPMENT FINANCE, LLC		
2018/07/06	26437057	Continuation	HEWLETT-PACKARD FINANCIAL SERVICES COMPANY		
2018/06/22	180008649330	Continuation	SUNTRUST EQUIPMENT FINANCE & LEASING CORP.		
2018/06/04	180007580323	Amendment	BANC OF AMERICA LEASING & CAPITAL, LLC		
2018/06/04	180007580626	Amendment	BANC OF AMERICA LEASING & CAPITAL, LLC		
2018/01/31	180001375723	Termination	PNC EQUIPMENT FINANCE, LLC		
2017/06/21	170008531825	Continuation	CHASE EQUIPMENT LEASING INC.		
2017/06/13	170008103416	Termination	CROWN CREDIT COMPANY		
2017/05/05	170006222416	Continuation	PNC EQUIPMENT FINANCE, LLC		
2017/01/03	170000018211	Original	IBM CREDIT LLC	Computer Equipment	Fixed
2016/12/19	160016292626	Continuation	PNC EQUIPMENT FINANCE, LLC		
2016/11/15	160014958734	Continuation	PNC EQUIPMENT FINANCE, LLC		
2016/10/25	160013971122	Original	IBM CREDIT LLC	Computer Equipment	Fixed

Filing Date	Filing No.	Filing Type	Secured Party	Collateral	Asset Type
2016/08/16	160010918423	Continuation	PNC EQUIPMENT FINANCE, LLC		
2016/08/01	160010149116	Original	IBM CREDIT LLC		
2016/07/05	160008889538	Original	IBM CREDIT LLC	Computer Equipment	Fixed
2016/06/23	160008395833	Original	IBM CREDIT LLC	Computer Equipment	Fixed
2016/05/18	20161390360	Continuation	PNC EQUIPMENT FINANCE, LLC		
2016/04/13	2016 2184099	Original	DOCUMATION	Business Machinery / Equipment, Computer Equipment, Communications Equipment	Fixed
2016/02/14	160002032007	Original	IBM CREDIT LLC	Computer Equipment	Fixed
2015/08/31	150011024210	Original	CROWN CREDIT COMPANY	Equipment, Vehicles, Accounts, Contract Rights, Chattel Paper, General Intangibles	Both Fixed and Current
2015/07/01	150008384730	Original	IBM CREDIT LLC	Computer Equipment	Fixed
2015/05/28	150006800418	Termination	THE FIFTH THIRD LEASING COMPANY		
2015/05/28	150006800519	Termination	THE FIFTH THIRD LEASING COMPANY		

BACK TO TABLE OF CONTENTS

Financial Health

Key Indicators USD (mil)

	Quarter Ending 31-Mar-2019	Quarter Ending Yr Ago	Annual Year End 31-Dec-2018	1 Year Growth	3 Year Growth	5 Year Growth
Total Revenue	1,502.0	4.31%	5,823.0	2.23%	3.48%	3.88%
Operating Income	363.0	-3.46%	1,526.0	0.26%	5.19%	7.54%
Net Income	225.0	-46.81%	1,187.0	-4.74%	18.55%	12.87%
Basic EPS	0.58	-43.14%	2.93	-0.68%	24.43%	18.86%
Capital Expenditures	-98.0	27.27%	-360.0	25.44%	0.09%	8.81%
Cash from Operating Activities	373.0	0.27%	1,552.0	4.65%	4.86%	8.36%
Free Cash Flow	275.0	-6.78%	1,192.0	-0.33%	6.49%	8.22%
Total Assets	11,676.0	14.84%	11,262.0	9.46%	6.43%	3.43%
Total Liabilities	9,282.0	28.99%	8,969.0	18.67%	10.31%	8.63%
Total Long-Term Debt	5,868.0	27.48%	5,955.0	21.61%	11.56%	9.66%
Employees	-	-	24000	0.00%	2.94%	2.71%
Total Common Shares Outstanding	392.3	-4.55%	392.5	-5.47%	-4.49%	-5.23%
Market Cap	34,613.5	18.05%	28,844.8	5.55%	11.85%	13.73%

Key Ratios

	31-Dec-2018	31-Dec-2017	31-Dec-2016	31-Dec-2015	31-Dec-2014
Profitability					
Gross Margin	47.30%	46.91%	46.25%	44.63%	43.13%
Operating Margin	26.21%	26.72%	26.25%	24.95%	23.88%
Pretax Margin	26.70%	23.84%	23.16%	20.12%	20.67%
Net Profit Margin	20.38%	21.88%	16.89%	13.55%	14.88%
Financial Strength					
Current Ratio	1.11	1.02	0.95	1.00	0.97
Long-Term Debt/Equity	2.60	1.79	1.76	1.61	1.12
Total Debt/Equity	2.60	1.79	1.80	1.61	1.15
Interest Coverage	9.06	8.72	8.82	7.22	7.38
Management Effectiveness					
Return on Assets	11.02%	12.44%	9.75%	7.64%	8.01%
Return on Equity	47.25%	47.27%	35.76%	23.91%	21.92%
Efficiency					
Receivables Turnover	5.69	6.00	6.46	6.57	6.54
Asset Turnover	0.54	0.57	0.58	0.56	0.54

Market Valuation USD (mil)			
P/E Ratio	37.51	Price/Book	14.94
Revenue/Share	14.42	Book Value/Share	6.10
Enterprise Value	42,512.5	Market Cap	37,089.5

© 2019 Morningstar. All Rights Reserved.
Published by Dun & Bradstreet, inc., July 2019.

▲ BACK TO TABLE OF CONTENTS

Geographic Segments

Revenue USD (mil)

	31-Dec-18		31-Dec-17		31-Dec-16		31-Dec-15	
Outside the United States	349.4	6 %	284.8	5 %	275.3	5 %	-	-
Outside United States	-	-	-	-	-	-	315.2	6 %
United States	5,473.6	94 %	5,411.2	95 %	5,229.8	95 %	4,938.8	94 %
SegmentTotal	5,823.0	100 %	5,696.0	100 %	5,505.0	100 %	5,254.0	100 %

© 2019 Dun & Bradstreet, Inc. All rights reserved.
Published by Dun & Bradstreet, Inc., July 2019.

BACK TO TABLE OF CONTENTS

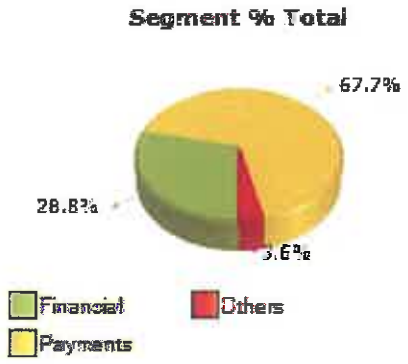
Business Segments

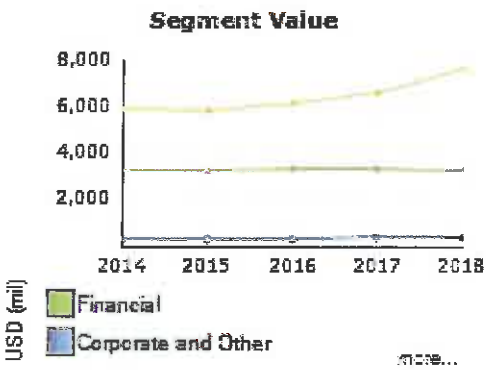
Total Assets

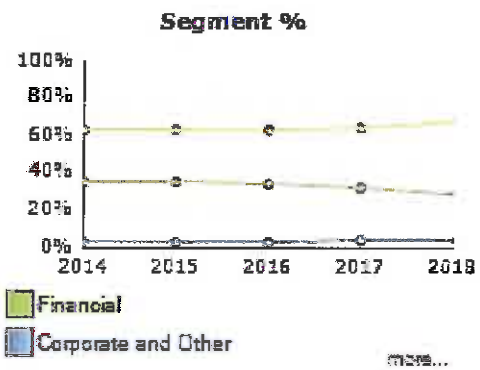
USD (mil)

	31-Dec-18		31-Dec-17		31-Dec-16		31-Dec-15		31-Dec-14	
Corporate and Other	400.0	3.6 %	384.0	3.7 %	313.0	3.2 %	265.0	2.8 %	262.0	2.8 %
Financial	3,240.0	28.8 %	3,309.0	32.2 %	3,287.0	33.7 %	3,242.0	34.7 %	3,225.0	34.5 %
Payments	7,622.0	67.7 %	6,596.0	64.1 %	6,143.0	63.1 %	5,833.0	62.5 %	5,850.0	62.7 %
SegmentTotal	11,262.0	100 %	10,289.0	100 %	9,743.0	100 %	9,340.0	100 %	9,337.0	100 %

Total Assets Charts







Revenue

USD (mil)

	31-Dec-18		31-Dec-17		31-Dec-16		31-Dec-15		31-Dec-14	
Corporate and Other	-39.0	-0.7 %	-68.0	-1.2 %	-62.0	-1.1 %	-51.0	-1 %	-48.0	-0.9 %
Financial	2,395.0	41.1 %	2,530.0	44.4 %	2,477.0	45 %	2,443.0	46.5 %	2,367.0	46.7 %
Payments	3,467.0	59.5 %	3,234.0	56.8 %	3,090.0	56.1 %	2,862.0	54.5 %	2,747.0	54.2 %
SegmentTotal	5,823.0	100 %	5,696.0	100 %	5,505.0	100 %	5,254.0	100 %	5,066.0	100 %

Operating Income

USD (mil)

	31-Dec-18		31-Dec-17		31-Dec-16		31-Dec-15		31-Dec-14	
Corporate and Other	-167.0	-9.5 %	-351.0	-22.9 %	-321.0	-22.2 %	-355.0	-27.1 %	-331.0	-27.4 %
Financial	798.0	45.5 %	849.0	55.4 %	823.0	57 %	826.0	63 %	773.0	63.9 %
Payments	1,122.0	64 %	1,034.0	67.5 %	943.0	65.3 %	840.0	64.1 %	768.0	63.5 %
SegmentTotal	1,753.0	100 %	1,532.0	100 %	1,445.0	100 %	1,311.0	100 %	1,210.0	100 %

Capital Expenditure

USD (mil)

	31-Dec-15		31-Dec-14	
Corporate and Other	-10.0	2.8 %	-9.0	3.1 %
Financial	-119.0	33.1 %	-107.0	36.6 %
Payments	-230.0	64.1 %	-176.0	60.3 %
SegmentTotal	-359.0	100 %	-292.0	100 %

© 2019 Dun & Bradstreet, Inc. All rights reserved.
Published by Dun & Bradstreet, Inc., July 2019.

BACK TO TABLE OF CONTENTS

Annual Ratios

Financials In: USD Millions

Except for share items (millions) and per share items (actual units)

	31-Dec-2018	31-Dec-2017	31-Dec-2016	31-Dec-2015	31-Dec-2014
Financial Strength					
Current Ratio	1.11	1.02	0.95	1.00	0.97
Quick/Acid Test Ratio	0.73	0.68	0.66	0.72	0.73
Working Capital	214.0	37.0	-92.0	4.0	-42.0
Long-Term Debt/Equity	2.60	1.79	1.76	1.61	1.12
Total Debt/Equity	2.60	1.79	1.80	1.61	1.15
Long-Term Debt/Total Capital	0.72	0.64	0.64	0.62	0.53
Total Debt/Total Capital	0.72	0.64	0.65	0.62	0.54
Interest Coverage	9.06	8.72	8.82	7.22	7.38
Payout Ratio	0.00%	0.00%	0.00%	0.00%	0.00%
Effective Tax Rate	24.31%	11.63%	38.59%	35.67%	36.68%
Total Capitalization	8,248.0	7,628.0	7,008.0	6,948.0	6,993.0
Efficiency					
Asset Turnover	0.54	0.57	0.58	0.56	0.54
Receivables Turnover	5.69	6.00	6.46	6.57	6.54
Days Receivables Outstanding	64.12	60.84	56.49	55.58	55.80
Revenue/Employee	242,625	237,333	239,348	238,818	241,238
Operating Income/Employee	63,583	63,417	62,826	59,591	57,619
EBITDA/Employee	96,000	82,417	80,826	74,727	76,905
Profitability					
Gross Margin	47.30%	46.91%	46.25%	44.63%	43.13%
Operating Margin	26.21%	26.72%	26.25%	24.95%	23.88%
EBITDA Margin	39.57%	34.73%	33.77%	31.29%	31.88%
EBIT Margin	30.02%	26.93%	26.12%	23.35%	23.90%
Pretax Margin	26.70%	23.84%	23.16%	20.12%	20.67%
Net Profit Margin	20.38%	21.88%	16.89%	13.55%	14.88%
COGS/Revenue	52.70%	53.09%	53.75%	55.37%	56.87%
SG&A Expense/Revenue	21.09%	20.19%	20.00%	19.68%	19.25%
Management Effectiveness					
Return on Assets	11.02%	12.44%	9.75%	7.64%	8.01%
Return on Equity	47.25%	47.27%	35.76%	23.91%	21.92%
Valuation					
Free Cash Flow/Share	2.64	2.60	2.52	1.95	4.17
Operating Cash Flow/Share	3.46	3.23	3.16	2.69	5.34
Current Market Multiples					

Market Cap/Earnings (TTM)	35.91
Market Cap/Equity (MRQ)	14.94
Market Cap/Revenue (TTM)	6.08
Market Cap/EBIT (TTM)	24.55
Market Cap/EBITDA (TTM)	17.67
Enterprise Value/Earnings (TTM)	41.35
Enterprise Value/Equity (MRQ)	17.21
Enterprise Value/Revenue (TTM)	7.00
Enterprise Value/EBIT (TTM)	28.28
Enterprise Value/EBITDA (TTM)	20.34

© 2019 Morningstar. All Rights Reserved.
Published by Dun & Bradstreet, Inc., July 2019.

BACK TO TABLE OF CONTENTS

Ratio Comparisons

Ratio Comparisons as of 28-Jun-2019

Traded: NASDAQ: FISV
Industry: Business Services
Sector: Industrials

	Company	Industry	Sector
Valuation Ratios			
P/E Ratio	37.51	46.51	24.27
Price/Revenue	6.32	2.91	1.54
Price/Book	14.94	5.32	3.87
Price to Cash Flow per Share	23.95	20.53	5.40
Price to Free Cash Flow per Share	31.74	28.49	12.25
Dividends			
Dividend Yield	-	0.89%	1.68%
Payout Ratio	0.00%	69.71%	48.25%
Financial Strength			
Quick/Acid Test Ratio	0.73	0.44	0.86
Current Ratio	1.11	1.11	1.36
Total Debt/Equity	2.60	1.13	1.33
Profitability Ratios (%)			
Gross Margin	47.30%	36.64%	26.77%
EBITDA Margin (TTM)	34.41%	17.48%	14.75%
Operating Margin (TTM)	25.71%	10.68%	10.01%
Pretax Margin (TTM)	21.24%	7.77%	8.11%
Net Profit Margin (TTM)	16.93%	7.70%	7.55%
Effective Tax Rate (TTM)	21.52%	22.97%	21.09%
Management Effectiveness (%)			
Return on Assets (TTM)	9.06%	3.28%	4.47%
Return on Average Investment (TTM)	14.54%	12.76%	12.42%
Return on Equity (TTM)	36.87%	11.53%	16.54%
Efficiency			
Revenue/Employee (TTM)	245,208.33	129,814.03	265,352.66
Receivables Turnover (TTM)	6.12	4.95	5.07
Inventory Turnover (TTM)	-	12.17	5.67
Asset Turnover (TTM)	0.54	0.53	0.70

© 2019 Morningstar. All Rights Reserved.

Published by Dun & Bradstreet, Inc., July 2019.

BACK TO TABLE OF CONTENTS

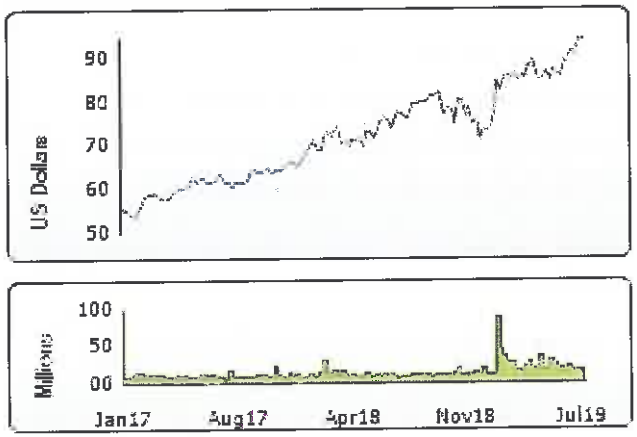
Stock Report

Stock Snapshot

Traded: NASDAQ: FISV
As of 12-Jul-2019 (Financials in: US Dollars)

Recent Price	94.51	**EPS**	2.43
52 Week High	94.89	**Price/Sales**	6.55
52 Week Low	68.45	**Price/Earnings**	38.89
Avg. Volume (mil)	3.50	**Price/Book**	15.49
Market Value (mil)	37,089.49	**Beta**	0.79

2 Year Weekly End Price & Volume



Stock History

Market Cap History USD (mil)

	31-Mar-19	% Chg	31-Dec-18	% Chg	30-Sep-18	% Chg	30-Jun-18	% Chg	31-Mar-18	% Chg
Total Common Shares Outstanding	392	-0.1	393	-2.1	401	-1.3	406	-1.2	411	-1.0
Market Cap	34,613.5	20.0	28,844.8	-13.5	33,357.9	10.0	30,335.2	3.5	29,320.7	7.3

Yearly Price History

	2019	% Chg	2018	% Chg	2017	% Chg	2016	% Chg	2015	% Chg
High Price	94.89	14.6	82.79	24.2	66.68	19.6	55.76	14.1	48.88	33.4
Low Price	68.45	9.1	62.76	20.1	52.26	22.0	42.82	23.9	34.57	28.8
Year End Price	94.51	28.6	73.49	12.1	65.57	23.4	53.14	16.2	45.73	28.9

Monthly Price History

Price Ending Date	Open	High	Low	Close	Volume
12-Jul-19	94.10	94.89	92.28	94.51	13,652,330
28-Jun-19	86.09	92.29	82.24	91.16	61,783,287

Price Ending Date	Open	High	Low	Close	Volume
31-May-19	85.75	89.66	81.62	85.86	85,641,422
30-Apr-19	88.98	91.19	84.32	87.24	92,249,417
29-Mar-19	85.11	88.65	83.31	88.28	79,508,944
28-Feb-19	82.63	86.29	82.29	84.69	81,612,530
31-Jan-19	73.49	85.65	68.45	82.93	170,669,840
31-Dec-18	79.58	80.07	68.55	73.49	45,798,933
30-Nov-18	74.09	80.62	73.51	79.13	45,932,561
31-Oct-18	82.66	82.79	75.74	79.30	46,527,384
28-Sep-18	80.07	82.41	79.24	82.38	32,621,542
31-Aug-18	75.48	80.45	73.84	80.07	40,771,372
31-Jul-18	73.70	78.21	73.54	75.48	29,070,266
29-Jun-18	73.01	76.98	72.12	74.09	37,326,676
31-May-18	70.85	73.56	68.43	72.60	39,354,031
30-Apr-18	71.04	72.62	69.66	70.86	32,080,276
29-Mar-18	71.93	74.46	69.77	71.31	45,184,593
28-Feb-18	70.34	73.72	62.76	71.70	62,040,348
31-Jan-18	65.57	72.10	64.91	70.42	38,467,226
29-Dec-17	65.25	66.68	64.10	65.57	30,379,230
30-Nov-17	62.00	65.93	60.19	65.73	45,753,376
31-Oct-17	64.61	65.10	63.16	64.72	34,683,622
29-Sep-17	62.10	64.81	60.59	64.48	31,970,122
31-Aug-17	64.29	64.68	59.85	61.86	35,897,566
31-Jul-17	61.38	64.29	60.37	64.25	27,030,512
30-Jun-17	62.70	63.55	60.19	61.17	39,375,334
31-May-17	59.75	62.67	58.67	62.64	34,568,480
28-Apr-17	57.75	61.46	57.48	59.57	29,869,852
31-Mar-17	58.09	59.15	56.65	57.66	40,142,948
28-Feb-17	53.57	58.35	52.26	57.70	46,402,538
31-Jan-17	53.14	55.75	53.14	53.72	34,648,968
30-Dec-16	52.28	54.56	51.30	53.14	37,704,006
30-Nov-16	49.37	53.95	48.53	52.31	57,285,584
31-Oct-16	49.55	50.50	46.41	49.24	51,615,354
30-Sep-16	51.55	52.34	48.87	49.74	43,461,896
31-Aug-16	55.08	55.50	50.50	51.53	46,968,168
29-Jul-16	54.26	55.76	53.99	55.18	33,478,050
30-Jun-16	52.63	54.43	50.80	54.37	44,479,158
31-May-16	48.80	53.07	48.76	52.67	43,545,214
29-Apr-16	51.18	51.77	48.17	48.86	40,893,896
31-Mar-16	48.36	51.44	47.83	51.29	49,585,140
29-Feb-16	46.78	49.86	45.25	47.82	62,347,556
29-Jan-16	45.73	47.32	42.82	47.28	51,034,416
31-Dec-15	48.27	48.88	45.59	45.73	56,408,788
30-Nov-15	48.43	48.76	47.11	48.12	45,788,928
30-Oct-15	43.46	48.71	42.71	48.26	51,463,168
30-Sep-15	41.72	44.61	41.20	43.31	54,560,554

Price Ending Date	Open	High	Low	Close	Volume
31-Aug-15	43.43	45.27	38.98	42.64	51,991,032
31-Jul-15	41.62	44.39	41.58	43.43	50,243,894
30-Jun-15	40.33	43.20	39.51	41.42	55,976,092
29-May-15	39.07	40.83	38.54	40.08	40,574,968
30-Apr-15	39.69	40.22	38.46	38.80	35,234,574
31-Mar-15	39.27	40.49	38.17	39.70	44,813,740
27-Feb-15	36.38	39.78	35.89	39.04	48,250,690
30-Jan-15	35.49	37.31	34.57	36.27	46,093,810
31-Dec-14	35.61	36.64	34.03	35.49	57,649,492
28-Nov-14	34.87	35.96	34.57	35.75	43,255,216
31-Oct-14	32.27	35.04	30.28	34.74	58,853,382
30-Sep-14	32.24	33.06	31.73	32.32	34,247,796
29-Aug-14	30.78	32.41	30.27	32.24	41,094,828
31-Jul-14	30.31	31.55	29.84	30.84	38,602,746

© 2019 Morningstar. All Rights Reserved.

Published by Dun & Bradstreet, Inc., July 2019.

BACK TO TABLE OF CONTENTS

Annual Income (Standardized)

Financials In: USD Millions

Except for share items (millions) and per share items (actual units)

	31-Dec-2018	31-Dec-2017	31-Dec-2016	31-Dec-2015	31-Dec-2014
Period Length	12 Months	12 Months	12 Months	12 Months	12 Months
UpdateType/Date	**Filed 21-Feb-2019**	**Filed 21-Feb-2019**	**Filed 21-Feb-2019**	**Filed 22-Feb-2018**	**Filed 23-Feb-2017**
Filed Currency	USD	USD	USD	USD	USD
Exchange Rate	1	1	1	1	1
Auditor	Deloitte & Touche LLP	Deloitte & Touche LLP	Deloitte & Touche LLP	Deloitte & Touche LLP	Deloitte & Touche LLP
Auditor Opinion	Unqualified with Explanation	Unqualified	Unqualified	Unqualified	Unqualified
Operating Revenue	5,823.0	5,696.0	5,505.0	5,254.0	5,066.0
Total Revenue	**5,823.0**	**5,696.0**	**5,505.0**	**5,254.0**	**5,066.0**
Cost of Revenue	3,069.0	3,024.0	2,959.0	2,909.0	2,881.0
Gross Profit	**2,754.0**	**2,672.0**	**2,546.0**	**2,345.0**	**2,185.0**
Selling, General and Administrative Expenses	**1,228.0**	**1,150.0**	**1,101.0**	**1,034.0**	**975.0**
Total Operating Expense	**1,228.0**	**1,150.0**	**1,101.0**	**1,034.0**	**975.0**
Operating Income	**1,526.0**	**1,522.0**	**1,445.0**	**1,311.0**	**1,210.0**
Interest Income - Non-Operating	-	-	-	1.0	1.0
Interest Expense - Non-Operating	193.0	176.0	163.0	170.0	164.0
Net Non-Operating Interest Income (Expense)	**-193.0**	**-176.0**	**-163.0**	**-169.0**	**-163.0**
Gain on Sale of Business	227.0	10.0	-	-	-
Other Special Charges	14.0	-	-	85.0	-
Special Income (Charges)	213.0	10.0	-	-85.0	-
Other Non-Operating Income (Expenses)	9.0	2.0	-7.0	-	-
Other Income (Expense)	**222.0**	**12.0**	**-7.0**	**-85.0**	-
Income Before Tax	**1,555.0**	**1,358.0**	**1,275.0**	**1,057.0**	**1,047.0**
Total Income Tax	378.0	158.0	492.0	377.0	384.0
Income After Tax	**1,177.0**	**1,200.0**	**783.0**	**680.0**	**663.0**
Equity In Affiliates	10.0	32.0	147.0	32.0	91.0
Net Income from Continuing Operations	**1,187.0**	**1,232.0**	**930.0**	**712.0**	**754.0**
Discontinued Operations	-	14.0	-	-	-

	31-Dec-2018	31-Dec-2017	31-Dec-2016	31-Dec-2015	31-Dec-2014
Net Income	**1,187.0**	**1,246.0**	**930.0**	**712.0**	**754.0**
Net Income Available to Common Stockholders	**1,187.0**	**1,246.0**	**930.0**	**712.0**	**754.0**
Basic EPS	2.93	2.95	2.11	1.52	1.52
Basic EPS from Continuing Operations	2.93	2.92	2.11	1.52	1.52
Basic EPS from Discontinued Operations	-	0.03	-	-	-0.01
Diluted EPS	2.87	2.89	2.08	1.50	1.49
Diluted EPS from Continuing Operations	2.87	2.86	2.08	1.50	1.50
Diluted EPS from Discontinued Operations	-	0.03	-	-	-0.01
Basic Average Shares	405.5	422.3	440.6	467.8	497.2
Diluted Average Shares	413.7	431.3	447.8	476.0	505.4
Interest Income	-	-	-	1.0	1.0
Interest Expense	193.0	176.0	163.0	170.0	164.0
Net Interest Income	-193.0	-176.0	-163.0	-169.0	-163.0
Net Income Including Non-Controlling Interests	1,187.0	1,246.0	930.0	712.0	754.0
Net Income from Continuing and Discontinued Operations	1,187.0	1,246.0	930.0	712.0	754.0
Normalized Income	1,025.8	1,223.2	930.0	766.7	754.0
Basic EPS from Continuing & Discontinued Operations	2.93	2.95	2.11	1.52	1.52
Diluted EPS from Continuing & Discontinued Operations	2.87	2.89	2.08	1.50	1.49
Net Income Before Extraord Items	1,187.0	1,232.0	930.0	712.0	754.0
Total Unusual Items	213.0	10.0	-	-85.0	-
Total Unusual Items Excluding Goodwill	213.0	10.0	-	-85.0	-
Tax Rate	24.30%	11.60%	38.60%	35.70%	36.60%
Tax Effect of Unusual Items	51.8	1.2	-	-30.3	-
Basic Normalized EPS	2.53	2.90	2.11	1.64	1.52
Diluted Normalized EPS	2.48	2.84	2.08	1.61	1.50
EBITDA	2,304.0	1,978.0	1,859.0	1,644.0	1,615.0
Normalized EBITDA	2,091.0	1,968.0	1,859.0	1,729.0	1,615.0
Reconciled Cost of Revenue	3,069.0	3,024.0	2,959.0	2,909.0	2,881.0
Reconciled Depreciation	556.0	444.0	421.0	417.0	404.0
EBIT	1,748.0	1,534.0	1,438.0	1,227.0	1,211.0

© 2019 Morningstar. All Rights Reserved.
Published by Dun & Bradstreet, Inc., July 2019.

BACK TO TABLE OF CONTENTS

Interim Income (Standardized)

Financials In: USD Millions

Except for share items (millions) and per share items (actual units)

	31-Mar-2019	31-Dec-2018	30-Sep-2018	30-Jun-2018	31-Mar-2018
Period Length	3 Months	3 Months	3 Months	3 Months	3 Months
UpdateType/Date	Filed 01-May-2019	Filed 31-Dec-2018	Filed 01-Nov-2018	Filed 01-Aug-2018	Filed 01-May-2019
Filed Currency	USD	USD	USD	USD	USD
Exchange Rate	1	1	1	1	1
Operating Revenue	1,502.0	1,551.0	1,412.0	1,420.0	1,440.0
Total Revenue	**1,502.0**	**1,551.0**	**1,412.0**	**1,420.0**	**1,440.0**
Cost of Revenue	798.0	822.0	749.0	739.0	759.0
Gross Profit	**704.0**	**729.0**	**663.0**	**681.0**	**681.0**
Selling, General and Administrative Expenses	**341.0**	**298.0**	**305.0**	**320.0**	**305.0**
Total Operating Expense	**341.0**	**298.0**	**305.0**	**320.0**	**305.0**
Operating Income	**363.0**	**431.0**	**358.0**	**361.0**	**376.0**
Interest Expense - Non-Operating	59.0	56.0	47.0	45.0	45.0
Other Finance Cost	59.0	-	-	-	-
Net Non-Operating Interest Income (Expense)	**-118.0**	**-56.0**	**-47.0**	**-45.0**	**-45.0**
Gain on Sale of Business	10.0	-	-2.0	-3.0	232.0
Other Special Charges	-	6.0	8.0	-	-
Special Income (Charges)	10.0	-6.0	-10.0	-3.0	232.0
Other Non-Operating Income (Expenses)	3.0	3.0	3.0	3.0	-
Other Income (Expense)	**13.0**	**-3.0**	**-7.0**	**-**	**232.0**
Income Before Tax	**258.0**	**372.0**	**304.0**	**316.0**	**563.0**
Total Income Tax	31.0	88.0	78.0	72.0	140.0
Income After Tax	**227.0**	**284.0**	**226.0**	**244.0**	**423.0**
Equity In Affiliates	-2.0	2.0	1.0	7.0	-
Net Income from Continuing Operations	**225.0**	**286.0**	**227.0**	**251.0**	**423.0**
Net Income	**225.0**	**286.0**	**227.0**	**251.0**	**423.0**
Net Income Available to Common Stockholders	**225.0**	**286.0**	**227.0**	**251.0**	**423.0**

	31-Mar-2019	31-Dec-2018	30-Sep-2018	30-Jun-2018	31-Mar-2018
Basic EPS	0.58	0.73	0.56	0.61	1.02
Basic EPS from Continuing Operations	0.58	0.73	0.56	0.61	1.02
Diluted EPS	0.56	0.71	0.55	0.60	1.00
Diluted EPS from Continuing Operations	0.56	0.71	0.55	0.60	1.00
Basic Average Shares	391.7	396.8	403.8	408.4	413.1
Diluted Average Shares	399.1	405.0	412.0	416.4	421.6
Interest Expense	59.0	56.0	47.0	45.0	45.0
Net Interest Income	-118.0	-56.0	-47.0	-45.0	-45.0
Net Income Including Non-Controlling Interests	225.0	286.0	227.0	251.0	423.0
Net Income from Continuing and Discontinued Operations	225.0	286.0	227.0	251.0	423.0
Normalized Income	216.2	290.5	234.5	253.3	248.8
Basic EPS from Continuing & Discontinued Operations	0.58	0.73	0.56	0.61	1.02
Diluted EPS from Continuing & Discontinued Operations	0.56	0.71	0.55	0.60	1.00
Net Income Before Extraord Items	225.0	286.0	227.0	251.0	423.0
Total Unusual Items	10.0	-6.0	-10.0	-3.0	232.0
Total Unusual Items Excluding Goodwill	10.0	-6.0	-10.0	-3.0	232.0
Tax Rate	11.90%	24.31%	25.40%	23.00%	24.90%
Tax Effect of Unusual Items	1.2	-1.5	-2.5	-0.7	57.8
Basic Normalized EPS	0.56	0.74	0.58	0.62	0.60
Diluted Normalized EPS	0.54	0.72	0.57	0.61	0.59
EBITDA	462.0	578.0	487.0	498.0	741.0
Normalized EBITDA	452.0	584.0	497.0	501.0	509.0
Reconciled Cost of Revenue	798.0	822.0	749.0	739.0	759.0
Reconciled Depreciation	145.0	150.0	136.0	137.0	133.0
EBIT	317.0	428.0	351.0	361.0	608.0

© 2019 Morningstar. All Rights Reserved.
Published by Dun & Bradstreet, Inc., July 2019.

BACK TO TABLE OF CONTENTS

Annual Balance (Standardized)

Financials In: USD Millions

Except for share items (millions) and per share items (actual units)

	31-Dec-2018	31-Dec-2017	31-Dec-2016	31-Dec-2015	31-Dec-2014
Period Length					
UpdateType/Date	**Filed 21-Feb-2019**	**Filed 21-Feb-2019**	**Filed 21-Feb-2019**	**Filed 22-Feb-2018**	**Filed 23-Feb-2017**
Filed Currency	USD	USD	USD	USD	USD
Exchange Rate	1	1	1	1	1
Auditor	Deloitte & Touche LLP	Deloitte & Touche LLP	Deloitte & Touche LLP	Deloitte & Touche LLP	Deloitte & Touche LLP
Auditor Opinion	Unqualified with Explanation	Unqualified	Unqualified	Unqualified	Unqualified
Cash and Cash Equivalents	415.0	325.0	300.0	275.0	294.0
Cash, Cash Equivalents and Short-Term Investments	**415.0**	**325.0**	**300.0**	**275.0**	**294.0**
Accounts Receivable	1,049.0	997.0	902.0	802.0	798.0
Total Receivables	**1,049.0**	**997.0**	**902.0**	**802.0**	**798.0**
Assets Held For Sale - Current	-	50.0	-	-	-
Prepaid Assets	760.0	603.0	526.0	429.0	352.0
Total Current Assets	**2,224.0**	**1,975.0**	**1,728.0**	**1,506.0**	**1,444.0**
Land and Improvements	10.0	13.0	19.0	19.0	23.0
Buildings and Improvements	256.0	255.0	256.0	253.0	209.0
Machinery and Equipment	961.0	908.0	876.0	833.0	822.0
Property/Plant/Equipment - Gross	1,227.0	1,176.0	1,151.0	1,105.0	1,054.0
Accumulated Depreciation	-829.0	-786.0	-746.0	-709.0	-737.0
Property/Plant/Equipment - Net	**398.0**	**390.0**	**405.0**	**396.0**	**317.0**
Goodwill	5,702.0	5,590.0	5,373.0	5,200.0	5,209.0
Other Intangible Assets	2,143.0	1,882.0	1,833.0	1,872.0	2,003.0
Goodwill and Other Intangible Assets	**7,845.0**	**7,472.0**	**7,206.0**	**7,072.0**	**7,212.0**
Non-Current Accounts Receivable	419.0	84.0	-	-	-
Other Long-Term Assets	376.0	368.0	404.0	366.0	335.0
Total Non-Current Assets	**9,038.0**	**8,314.0**	**8,015.0**	**7,834.0**	**7,864.0**
Total Assets	**11,262.0**	**10,289.0**	**9,743.0**	**9,340.0**	**9,308.0**
Accounts Payable	127.0	80.0	110.0	74.0	61.0
Income Taxes Payable	-	-	184.0	-	-
Total Tax Payable	-	-	184.0	-	-
Payables	**127.0**	**80.0**	**294.0**	**74.0**	**61.0**

	31-Dec-2018	31-Dec-2017	31-Dec-2016	31-Dec-2015	31-Dec-2014
Accrued Expenses	736.0	600.0	539.0	424.0	391.0
Current Debt	4.0	3.0	95.0	5.0	92.0
Current Debt and Capital Lease Obligation	**4.0**	**3.0**	**95.0**	**5.0**	**92.0**
Customer Advances	944.0	1,057.0	892.0	803.0	750.0
Current Deferred Liabilities	944.0	1,057.0	892.0	803.0	750.0
Total Current Liabilities	**2,010.0**	**1,938.0**	**1,820.0**	**1,502.0**	**1,486.0**
Long-Term Debt	5,955.0	4,897.0	4,467.0	4,288.0	3,698.0
Long-Term Debt and Capital Lease Obligation	5,955.0	4,897.0	4,467.0	4,288.0	3,698.0
Deferred Taxes - Non-Current Liabilities	745.0	552.0	762.0	726.0	700.0
Non-Current Deferred Revenue	89.0	54.0	-	-	-
Non-Current Deferred Liabilities	834.0	606.0	762.0	726.0	700.0
Other Long-Term Liabilities	170.0	117.0	153.0	164.0	129.0
Total Non-Current Liabilities	**6,959.0**	**5,620.0**	**5,382.0**	**5,178.0**	**4,527.0**
Total Liabilities	**8,969.0**	**7,558.0**	**7,202.0**	**6,680.0**	**6,013.0**
Common Stock	8.0	8.0	4.0	4.0	4.0
Capital Stock	8.0	8.0	4.0	4.0	4.0
Retained Earnings (Accumulated Deficit)	11,635.0	10,240.0	8,994.0	8,064.0	7,352.0
Additional Paid-In Capital	1,057.0	1,031.0	1,020.0	952.0	897.0
Treasury Stock	-10,340.0	-8,494.0	-7,401.0	-6,286.0	-4,895.0
Gains (Losses) Not Affecting Retained Earnings	-67.0	-54.0	-76.0	-74.0	-63.0
Stockholders' Equity	**2,293.0**	**2,731.0**	**2,541.0**	**2,660.0**	**3,295.0**
Total Equity	**2,293.0**	**2,731.0**	**2,541.0**	**2,660.0**	**3,295.0**
Total Liabilities and Shareholders' Equity	**11,262.0**	**10,289.0**	**9,743.0**	**9,340.0**	**9,308.0**
Net Tangible Assets	-5,552.0	-4,741.0	-4,665.0	-4,412.0	-3,917.0
Working Capital	214.0	37.0	-92.0	4.0	-42.0
Invested Capital	8,252.0	7,631.0	7,103.0	6,953.0	7,085.0
Total Debt	5,959.0	4,900.0	4,562.0	4,293.0	3,790.0
Net Debt	5,544.0	4,575.0	4,262.0	4,018.0	3,496.0
Total Capitalization	8,248.0	7,628.0	7,008.0	6,948.0	6,993.0
Common Stock Equity	2,293.0	2,731.0	2,541.0	2,660.0	3,295.0
Total Common Shares Outstanding	392.5	415.2	431.0	450.6	480.6
Treasury Shares Number	398.9	376.0	360.4	340.8	310.8
Shares Issued	791.4	791.2	791.4	791.4	791.4
Tangible Book Value	-5,552.0	-4,741.0	-4,665.0	-4,412.0	-3,917.0

	31-Dec-2018	31-Dec-2017	31-Dec-2016	31-Dec-2015	31-Dec-2014
Employees	24,000	24,000	23,000	22,000	21,000

© 2019 Morningstar. All Rights Reserved.
Published by Dun & Bradstreet, Inc., July 2019.

BACK TO TABLE OF CONTENTS

Interim Balance (Standardized)

Financials In: USD Millions

Except for share items (millions) and per share items (actual units)

	31-Mar-2019	31-Dec-2018	30-Sep-2018	30-Jun-2018	31-Mar-2018
Period Length					
UpdateType/Date	**Filed 01-May-2019**	**Filed 31-Dec-2018**	**Filed 01-Nov-2018**	**Filed 01-Aug-2018**	**Filed 01-May-2019**
Filed Currency	USD	USD	USD	USD	USD
Exchange Rate	1	1	1	1	1
Cash and Cash Equivalents	452.0	415.0	673.0	348.0	382.0
Cash, Cash Equivalents and Short-Term Investments	**452.0**	**415.0**	**673.0**	**348.0**	**382.0**
Accounts Receivable	1,044.0	1,049.0	949.0	932.0	878.0
Total Receivables	**1,044.0**	**1,049.0**	**949.0**	**932.0**	**878.0**
Prepaid Assets	779.0	760.0	716.0	524.0	508.0
Total Current Assets	**2,275.0**	**2,224.0**	**2,338.0**	**1,804.0**	**1,768.0**
Land and Improvements	-	10.0	-	-	-
Buildings and Improvements	-	256.0	-	-	-
Machinery and Equipment	-	961.0	-	-	-
Property/Plant/Equipment - Gross	-	1,227.0	-	-	-
Accumulated Depreciation	-	-829.0	-	-	-
Property/Plant/Equipment - Net	**409.0**	**398.0**	**385.0**	**374.0**	**375.0**
Goodwill	5,703.0	5,702.0	5,450.0	5,456.0	5,454.0
Other Intangible Assets	2,117.0	2,143.0	1,802.0	1,833.0	1,855.0
Goodwill and Other Intangible Assets	**7,820.0**	**7,845.0**	**7,252.0**	**7,289.0**	**7,309.0**
Non-Current Accounts Receivable	435.0	419.0	410.0	398.0	401.0
Other Long-Term Assets	737.0	376.0	363.0	353.0	314.0
Total Non-Current Assets	**9,401.0**	**9,038.0**	**8,410.0**	**8,414.0**	**8,399.0**
Total Assets	**11,676.0**	**11,262.0**	**10,748.0**	**10,218.0**	**10,167.0**
Accounts Payable	98.0	127.0	97.0	95.0	81.0
Payables	**98.0**	**127.0**	**97.0**	**95.0**	**81.0**
Accrued Expenses	847.0	736.0	765.0	544.0	599.0
Current Debt	7.0	4.0	452.0	1.0	1.0
Current Debt and Capital Lease Obligation	**7.0**	**4.0**	**452.0**	**1.0**	**1.0**
Customer Advances	978.0	944.0	840.0	873.0	879.0
Current Deferred Liabilities	978.0	944.0	840.0	873.0	879.0
Other Current liabilities	78.0	-	-	-	-

	31-Mar-2019	31-Dec-2018	30-Sep-2018	30-Jun-2018	31-Mar-2018
Total Current Liabilities	**2,120.0**	**2,010.0**	**2,320.0**	**1,655.0**	**1,683.0**
Long-Term Debt	5,868.0	5,955.0	4,823.0	4,805.0	4,603.0
Long-Term Debt and Capital Lease Obligation	5,868.0	5,955.0	4,823.0	4,805.0	4,603.0
Deferred Taxes - Non-Current Liabilities	745.0	745.0	715.0	692.0	693.0
Non-Current Deferred Revenue	103.0	89.0	75.0	71.0	65.0
Non-Current Deferred Liabilities	848.0	834.0	790.0	763.0	758.0
Other Long-Term Liabilities	446.0	170.0	154.0	145.0	152.0
Total Non-Current Liabilities	**7,162.0**	**6,959.0**	**5,767.0**	**5,713.0**	**5,513.0**
Total Liabilities	**9,282.0**	**8,969.0**	**8,087.0**	**7,368.0**	**7,196.0**
Common Stock	8.0	8.0	8.0	8.0	8.0
Capital Stock	8.0	8.0	8.0	8.0	8.0
Retained Earnings (Accumulated Deficit)	11,860.0	11,635.0	11,349.0	11,122.0	10,871.0
Additional Paid-In Capital	1,034.0	1,057.0	1,045.0	1,023.0	1,005.0
Treasury Stock	-10,423.0	-10,340.0	-9,662.0	-9,237.0	-8,857.0
Gains (Losses) Not Affecting Retained Earnings	-85.0	-67.0	-79.0	-66.0	-56.0
Stockholders' Equity	**2,394.0**	**2,293.0**	**2,661.0**	**2,850.0**	**2,971.0**
Total Equity	**2,394.0**	**2,293.0**	**2,661.0**	**2,850.0**	**2,971.0**
Total Liabilities and Shareholders' Equity	**11,676.0**	**11,262.0**	**10,748.0**	**10,218.0**	**10,167.0**
Net Tangible Assets	-5,426.0	-5,552.0	-4,591.0	-4,439.0	-4,338.0
Working Capital	155.0	214.0	18.0	149.0	85.0
Invested Capital	8,269.0	8,252.0	7,936.0	7,656.0	7,575.0
Total Debt	5,875.0	5,959.0	5,275.0	4,806.0	4,604.0
Net Debt	5,423.0	5,544.0	4,602.0	4,458.0	4,222.0
Total Capitalization	8,262.0	8,248.0	7,484.0	7,655.0	7,574.0
Common Stock Equity	2,394.0	2,293.0	2,661.0	2,850.0	2,971.0
Total Common Shares Outstanding	392.3	392.5	401.0	406.1	411.0
Treasury Shares Number	399.1	398.9	390.4	385.3	380.4
Shares Issued	791.4	791.4	791.4	791.4	791.4
Tangible Book Value	-5,426.0	-5,552.0	-4,591.0	-4,439.0	-4,338.0
Employees	-	24,000	-	-	-

© 2019 Morningstar. All Rights Reserved.
Published by Dun & Bradstreet, Inc., July 2019.

BACK TO TABLE OF CONTENTS

Annual Cash Flow (Standardized)

Financials In: USD Millions

Except for share items (millions) and per share items (actual units)

	31-Dec-2018	31-Dec-2017	31-Dec-2016	31-Dec-2015	31-Dec-2014
Period Length	12 Months	12 Months	12 Months	12 Months	12 Months
UpdateType/Date	**Filed 21-Feb-2019**	**Filed 21-Feb-2019**	**Filed 21-Feb-2019**	**Filed 22-Feb-2018**	**Filed 23-Feb-2017**
Filed Currency	USD	USD	USD	USD	USD
Exchange Rate	1	1	1	1	1
Auditor	Deloitte & Touche LLP	Deloitte & Touche LLP	Deloitte & Touche LLP	Deloitte & Touche LLP	Deloitte & Touche LLP
Auditor Opinion	Unqualified with Explanation	Unqualified	Unqualified	Unqualified	Unqualified
Net Income from Continuing Operations	**1,187.0**	**1,232.0**	**930.0**	**712.0**	**754.0**
Gain (Loss) on Sale of Business	-227.0	-10.0	-	-	-
Equity in Net Earnings (Loss)	-10.0	-32.0	-147.0	-32.0	-91.0
Operating Gains (Losses)	**-223.0**	**-42.0**	**-147.0**	**53.0**	**-91.0**
Depreciation	393.0	285.0	263.0	223.0	200.0
Amortization of Intangibles	163.0	159.0	158.0	194.0	204.0
Amortization	163.0	159.0	158.0	194.0	204.0
Depreciation and Amortization	556.0	444.0	421.0	417.0	404.0
Depreciation, Amortization and Depletion	**556.0**	**444.0**	**421.0**	**417.0**	**404.0**
Deferred Income Tax	133.0	-247.0	21.0	20.0	3.0
Deferred Taxes	133.0	-247.0	21.0	20.0	3.0
Asset Impairment Charge	3.0	18.0	17.0	6.0	-
Stock-Based Compensation	73.0	63.0	68.0	65.0	49.0
Excess Tax Benefit from Stock-Based Compensation	-	-	-51.0	-38.0	-18.0
Other Non-Cash Items	-10.0	-4.0	-2.0	-1.0	-
Accounts Receivable	-108.0	-75.0	-88.0	-2.0	-42.0
Receivables	-108.0	-75.0	-88.0	-2.0	-42.0
Prepaid Expenses	-6.0	-37.0	-64.0	-66.0	-39.0
Accounts Payable	116.0	54.0	172.0	148.0	168.0
Payables	116.0	54.0	172.0	148.0	168.0
Payables/Accrued	116.0	54.0	172.0	148.0	168.0
Other Working Capital	-171.0	32.0	3.0	-4.0	9.0
Changes in Working Capital	**-169.0**	**-26.0**	**23.0**	**76.0**	**96.0**
Cash from Operating Activities	**1,552.0**	**1,483.0**	**1,431.0**	**1,346.0**	**1,307.0**
Capital Expenditure	-360.0	-287.0	-290.0	-359.0	-292.0
Purchase of Investments	-3.0	-10.0	-1.0	-4.0	-
Sale/Maturity of Investment	-	-	-	-	7.0

	31-Dec-2018	31-Dec-2017	31-Dec-2016	31-Dec-2015	31-Dec-2014
Investment, Net	**-3.0**	**-10.0**	**-1.0**	**-4.0**	**7.0**
Acquisition of Business	-712.0	-384.0	-265.0	-	-
Sale of Business	419.0	17.0	-	-	-
Net Acquisition (Sale) of Business	**-293.0**	**-367.0**	**-265.0**	-	-
Other Investing Cash Flow	-7.0	7.0	2.0	3.0	-1.0
Cash from Investing Activities	**-663.0**	**-657.0**	**-554.0**	**-360.0**	**-286.0**
Long-Term Debt Issued	5,039.0	2,310.0	2,126.0	3,121.0	604.0
Long-Term Debt Reduction	-4,005.0	-1,985.0	-1,863.0	-2,707.0	-653.0
Long-Term Debt, Net	1,034.0	325.0	263.0	414.0	-49.0
Issuance (Retirement) of Debt, Net	**1,034.0**	**325.0**	**263.0**	**414.0**	**-49.0**
Sale/Issuance of Common	75.0	78.0	79.0	71.0	53.0
Repurchase/Retirement of Common	-1,946.0	-1,223.0	-1,245.0	-1,522.0	-1,148.0
Common Stock, Net	**-1,871.0**	**-1,145.0**	**-1,166.0**	**-1,451.0**	**-1,095.0**
Other Financing Cash Flow	-5.0	-	51.0	32.0	18.0
Cash from Financing Activities	**-842.0**	**-820.0**	**-852.0**	**-1,005.0**	**-1,126.0**
Cash from Discontinued Operation	**43.0**	**19.0**	-	-	**-1.0**
Net Cash - Beginning Balance	**325.0**	**300.0**	**275.0**	**294.0**	**400.0**
Net Change in Cash	90.0	25.0	25.0	-19.0	-106.0
Net Cash - Ending Balance	**415.0**	**325.0**	**300.0**	**275.0**	**294.0**
Capital Expenditures	-360.0	-287.0	-290.0	-359.0	-292.0
Issuance of Capital Stock	75.0	78.0	79.0	71.0	53.0
Total Debt Issued	5,039.0	2,310.0	2,126.0	3,121.0	604.0
Total Debt Reduction	-4,005.0	-1,985.0	-1,863.0	-2,707.0	-653.0
Repurchase of Capital Stock	-1,946.0	-1,223.0	-1,245.0	-1,522.0	-1,148.0
Cash Taxes Paid	-	-	-	306.0	336.0
Cash Interest Paid	-	-	-	150.0	144.0
Free Cash Flow	1,192.0	1,196.0	1,141.0	987.0	1,015.0

© 2019 Morningstar. All Rights Reserved.
Published by Dun & Bradstreet, Inc., July 2019.

BACK TO TABLE OF CONTENTS

Interim Cash Flow (Standardized)

Financials In: USD Millions

Except for share items (millions) and per share items (actual units)

	31-Mar-2019	31-Dec-2018	30-Sep-2018	30-Jun-2018	31-Mar-2018
Period Length	3 Months	3 Months	3 Months	3 Months	3 Months
UpdateType/Date	**Filed 01-May-2019**	**Filed 31-Dec-2018**	**Filed 01-Nov-2018**	**Filed 01-Aug-2018**	**Filed 01-May-2019**
Filed Currency	USD	USD	USD	USD	USD
Exchange Rate	1	1	1	1	1
Net Income from Continuing Operations	**225.0**	**286.0**	**227.0**	**251.0**	**423.0**
Gain (Loss) on Sale of Business	-10.0	-	2.0	3.0	-232.0
Equity in Net Earnings (Loss)	2.0	-2.0	-1.0	-7.0	-
Operating Gains (Losses)	**-8.0**	**4.0**	**9.0**	**-4.0**	**-232.0**
Depreciation	100.0	107.0	96.0	97.0	93.0
Amortization of Intangibles	45.0	43.0	40.0	40.0	40.0
Amortization	45.0	43.0	40.0	40.0	40.0
Depreciation and Amortization	145.0	150.0	136.0	137.0	133.0
Depreciation, Amortization and Depletion	**145.0**	**150.0**	**136.0**	**137.0**	**133.0**
Deferred Income Tax	8.0	28.0	25.0	3.0	77.0
Deferred Taxes	8.0	28.0	25.0	3.0	77.0
Asset Impairment Charge	-	-	2.0	-	-
Stock-Based Compensation	19.0	19.0	18.0	17.0	19.0
Other Non-Cash Items	58.0	-	-	-	1.0
Accounts Receivable	6.0	-79.0	-18.0	-78.0	67.0
Receivables	6.0	-79.0	-18.0	-78.0	67.0
Prepaid Expenses	-26.0	57.0	1.0	-20.0	-44.0
Accounts Payable	-26.0	68.0	31.0	-21.0	38.0
Payables	-26.0	68.0	31.0	-21.0	38.0
Payables/Accrued	-26.0	68.0	31.0	-21.0	38.0
Other Working Capital	-28.0	47.0	-63.0	-45.0	-110.0
Changes in Working Capital	**-74.0**	**93.0**	**-49.0**	**-164.0**	**-49.0**
Cash from Operating Activities	**373.0**	**571.0**	**368.0**	**241.0**	**372.0**
Capital Expenditure	-98.0	-97.0	-94.0	-92.0	-77.0
Purchase of Investments	-	-3.0	2.0	-1.0	-1.0
Investment, Net	-	-3.0	**2.0**	-1.0	-1.0
Acquisition of Business	-	-712.0	-	-	-
Sale of Business	56.0	-	-	-	419.0
Net Acquisition (Sale) of Business	**56.0**	**-712.0**	-	-	**419.0**
Other Investing Cash Flow	6.0	6.0	-1.0	-2.0	-10.0

	31-Mar-2019	31-Dec-2018	30-Sep-2018	30-Jun-2018	31-Mar-2018
Cash from Investing Activities	**-36.0**	**-806.0**	**-93.0**	**-95.0**	**331.0**
Long-Term Debt Issued	587.0	1,412.0	2,466.0	652.0	509.0
Long-Term Debt Reduction	-680.0	-749.0	-1,999.0	-451.0	-806.0
Long-Term Debt, Net	-93.0	663.0	467.0	201.0	-297.0
Issuance (Retirement) of Debt, Net	**-93.0**	**663.0**	**467.0**	**201.0**	**-297.0**
Sale/Issuance of Common	32.0	15.0	16.0	16.0	28.0
Repurchase/Retirement of Common	-183.0	-692.0	-430.0	-397.0	-427.0
Common Stock, Net	**-151.0**	**-677.0**	**-414.0**	**-381.0**	**-399.0**
Other Financing Cash Flow	-56.0	-9.0	-3.0	-	-
Cash from Financing Activities	**-300.0**	**-23.0**	**50.0**	**-173.0**	**-696.0**
Cash from Discontinued Operation	-	-	-	**-7.0**	**50.0**
Net Cash - Beginning Balance	**415.0**	**673.0**	**348.0**	**382.0**	**325.0**
Net Change in Cash	37.0	-258.0	325.0	-34.0	57.0
Net Cash - Ending Balance	**452.0**	**415.0**	**673.0**	**348.0**	**382.0**
Capital Expenditures	-98.0	-97.0	-94.0	-92.0	-77.0
Issuance of Capital Stock	32.0	15.0	16.0	16.0	28.0
Total Debt Issued	587.0	1,412.0	2,466.0	652.0	509.0
Total Debt Reduction	-680.0	-749.0	-1,999.0	-451.0	-806.0
Repurchase of Capital Stock	-183.0	-692.0	-430.0	-397.0	-427.0
Cash Taxes Paid	-	-	82.0	-	-
Cash Interest Paid	-	-	14.0	-	-
Free Cash Flow	275.0	474.0	274.0	149.0	295.0

© 2019 Morningstar. All Rights Reserved.
Published by Dun & Bradstreet, Inc., July 2019.

BACK TO TABLE OF CONTENTS

dun & bradstreet

Supplier Qualifier Report

Print this Report

Copyright 2019 Dun & Bradstreet - Provided under contract for the exclusive use of subscriber 263159923

ATTN: **Name1**

Report Printed: APR 08 2019
In Date

BUSINESS INFORMATION

FISERV, INC.
FISERV
255 Fiserv Dr
Brookfield, WI 53045

This is a **headquarters** location.
Branch(es) or division(s) exist.

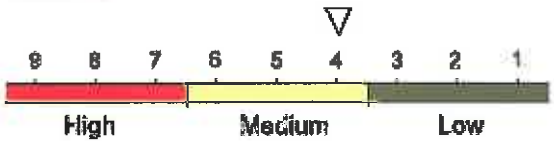
Mailing address:	PO Box 979 Brookfield, WI 53008
Telephone:	262 879-5000
Chief executive:	JEFFERY W YABUKI, PRES-CEO
Stock symbol:	FISV
Year started:	1984
Employs:	24,000 (65 here)

All amounts are displayed in local currency.

Financial statement date:	DEC 31 2018
Net worth F:	2,293,000,000
Gross revenue F:	5,823,000,000
History:	CLEAR
Financing:	SECURED
Financial condition:	GOOD

D-U-N-S® Number:	12-159-4832
D&B Rating:	**5A2**
Financial strength:	5A is **$50 million and over.**
Composite credit appraisal:	2 is **good.**
D&B Supplier Risk:	**4**

SUPPLIER EVALUATION RISK (SER) RATING FOR THIS FIRM : 4



D&B PAYDEX®

D&B PAYDEX: 73
When weighted by dollar amount, payments to suppliers average 11 days beyond terms.



d on up to 24 months of trade.

SUMMARY ANALYSIS

D&B Rating: **5A2**

Financial strength: 5A indicates **$50 million and over**.

Composite credit appraisal: 2 is **good**.

This credit rating was assigned because of D&B's assessment of the company's financial ratios and its cash flow. For more information, see the D&B Rating Key.

Below is an overview of the company's rating history since 01/01/91:

D&B Rating	Date Applied
5A2	03/01/11
5A3	05/02/08
5A2	06/07/06
5A3	03/16/01
--	09/06/95
5A2	03/24/93
5A3	01/01/91

The Summary Analysis section reflects information in D&B's file as of April 8, 2019.

RISK SCORE ANALYSIS

SER COMMENTARY:
- Change in net worth.
- Proportion of slow payment experiences to total number of payment experiences reported.
- Total Liabilities to Net Worth influencing the score.

PROBABILITY OF CEASED OPERATIONS/BECOMING INACTIVE

SUPPLIER EVALUATION RISK RATING: 4

The probability of ceased operations/becoming inactive indicates what percent of U.S. businesses is expected to cease operations or become inactive over next 12 months.

Probability of Supplier Ceased Operations/Becoming Inactive : 3.7% (370 PER 10,000)

Percentage of US business with same SER score : 13% (1,300 PER 10,000)

Average Probability of Supplier Ceased Operations/Becoming Inactive : 0.48% (48 PER 10,000)
- Average of Businesses in D&B's Supplier Database

CREDIT DELINQUENCY SCORE: 525

SPECIAL EVENTS

01/16/2019
ANNOUNCED MERGER/ACQUISITION: According to published reports, Fiserv, DUNS 121594832, (Brookfield, WI) announced that it has struck an agreement to acquire First Data, DUNS 604360081, (New York, NY) in an all-stock transaction valued at $22 billion. The deal has been approved by both companies boards but still needs to be accepted by shareholders and regulators. Under the deal terms, First Data shareholders will receive 0.303 Fiserv shares for each First Data share of common stock they own.

11/09/2018
PURCHASE OF ASSET: According to published reports, Fiserv, DUNS 121594832, (Brookfield, WI) announced that it finalized its acquisition of debit processing technology from U.S. Banks Elan Financial Services; a deal Fiserv first announced in September. Terms of the acquisition, which does not include the Elan credit card issuing and corporate payments businesses, were undisclosed.

09/27/2018
STOCK/BOND ISSUANCE/REDEMPTION/REPURCHASE: According to published reports, Fiserv, Inc. announced the expiration and results of the previously announced offer to purchase for cash any and all of its outstanding 4.625% Senior Notes due 2020, which expired at New York City time, on September 26, 2018. As of the Expiration

Time, $245,610,000 aggregate principal amount of Notes, or 54.58% of the aggregate principal amount of Notes outstanding, had been validly tendered and not validly withdrawn. This excludes $644,000 aggregate principal amount of Notes that remain subject to guaranteed delivery procedures. The complete terms and conditions of the Offer were set forth in an Offer to Purchase, dated September 20, 2018, and the related Letter of Transmittal.

09/26/2018
DUNCED PURCHASE OF ASSET: According to published reports, Fiserv, Inc., DUNS 121594832, (Brookfield, WI) announced it has agreed to acquire the debit card processing, ATM Managed Services and MoneyPass surcharge free network of Elan Financial Services, DUNS 024207002, (Aberdeen, OH).

09/20/2018
STOCK/BOND ISSUANCE/REDEMPTION/REPURCHASE: According to published reports, Fiserv, Inc. announced that it has commenced a cash tender offer for any and all of its outstanding 4.625% Senior Notes due 2020, on the terms and subject to the conditions set forth in the Offer to Purchase, dated as of the date hereof, the related Letter of Transmittal, and the related Notice of Guaranteed Delivery attached to the Offer to Purchase. As of September 20, 2018, there were $450,000,000 aggregate principal amount of Notes outstanding. The tender offer is referred to herein as the "Offer." The Offer to Purchase, the Letter of Transmittal and the Notice of Guaranteed Delivery are referred to herein collectively as the "Offer Documents.".

08/10/2018
STOCK/BOND ISSUANCE/REDEMPTION/REPURCHASE: According to published reports, Fiserv, Inc. announced that its Board of Directors has authorized it to repurchase 30 million shares of the company's common stock, which is in addition to the shares remaining available under the company's existing authorization.

05/22/2018
SALE OF ASSET: According to published reports, Fiserv Inc., DUNS 121594832, (Brookfield, WI) announced that it has sold a 55 percent interest of its Lending Solutions business to funds affiliated with Warburg Pincus LLC, DUNS 068236108, (New York, NY), retaining a 45 percent interest. The company received total sale proceeds of $419 million from the transaction in the quarter.

05/02/2018
EARNINGS UPDATE: According to published reports, comparative operating results for the 3 months ended March 31, 2018: Revenue of $1,440,000,000, Net Income of $423,000,000; compared to Revenue of $1,394,000,000, Net Income of $247,000,000 for the comparable period in the prior year.

CUSTOMER SERVICE

If you have questions about this report, please call our Customer Resource Center at 1.800.234.3867 from anywhere within the U.S. If you are outside the U.S. contact your local D&B office.

*** Additional Decision Support Available ***

Additional D&B products, monitoring services and specialized investigations are available to help you evaluate this company or its industry. Call Dun & Bradstreet's Customer Resource Center at 1.800.234.3867 from anywhere within the U.S. or visit our website at www.dnb.com.

HISTORY

The following information was reported **12/27/2018**:

Officer(s):
GLENN M RENWICK, CHB+
JEFFERY W YABUKI, PRES-CEO+
ROBERT W HAU, CFO-TREAS
LYNN S MCCREARY, CLO-SEC
BYRON VIELEHR, CHIEF ADM OFFICER

DIRECTOR(S): The officers identified by (+) and Alison Davis, Harry F DiSimone, John Y Kim, Dennis F Lynch, Denis J OLeary, Kim M Robak, JD Sherman and Doyle R Simons.

The Wisconsin Secretary of State's business registrations file showed that Fiserv, Inc. was registered as a Corporation on February 19, 1992, under the file registration number F024977.

Business started 1984.

Company was originally incorporated in Delaware in 1984 and reincorporated as a Wisconsin corporation in 1992.

The company's common stock is traded on the NASDAQ Global Select Market under the symbol "FISV". As of December 31, 2017, there were 1,883 shareholders of record of the company's common stock. As of March 7, 2018, those shareholders identified by the company as beneficially owning 5% or more of the outstanding shares were: T Rowe Price Associates, Inc (14.4%); The Vanguard Group, Inc (10.4%); and BlackRock, Inc (7.3%). As of the same

date, directors and officers as a group beneficially owns 1.7% of the outstanding shares.

RECENT EVENTS:

On October 31, 2018, the company acquired the debit card processing, ATM Managed Services, and Money Pass surcharge-free network of Elan Financial Services, a unit of U.S. Bancorp, for approximately $690 million, subject to post-closing adjustments.

On January 17, 2017, the company acquired Online Banking Solutions, Inc. With the acquisition, Online Banking Solutions, Inc. changed its name into SBO Group, Inc. and has remained to be a separate legal entity.

On March 29, 2018, Warburg Pincus LLC, through its affiliated funds has acquired 55% controlling interest of each of Fiserv Automotive Solutions, LLC and Fiserv LS LLC from Fiserv, Inc. With the acquisition, Fiserv Automotive Solutions, LLC and Fiserv LS LLC will now operate as subsidiaries of Warburg Pincus LLC. The total value of the transaction was approximately $395 million.

On January 10, 2018, the company completed the sale of its retail voucher business, MyVoucherCodes, acquired as part of the companys acquisition of Monitise in September 2017 for $50 million.

On September 1, 2017, the company completed its acquisition of Monitise plc.

On August 18, 2017, the company acquired Dovetail Group Limited.

On July 31, 2017, the company acquired the assets of PCLender, LLC.

On May 11, 2017, the company sold its Australian item processing business, which was reported within the Financial segment, for approximately $17 million.

On January 17, 2017, the company completed its acquisition of Online Banking Solutions, Inc.

In 2016, the company acquired the Convenience Pay Services business of Hewlett Packard Enterprise Company and completed its purchase of the Community Financial Services business of ACI Worldwide, Inc. for an aggregate purchase price of $265 million.

GLENN M RENWICK. Director since 2001. He serves as the company's Chairman of the Board. He is Executive Chairman of The Progressive Corporation and also served as its President and CEO from 2001 to 2016.

JEFFERY W YABUKI. Director since 2005. He has served as the company's President and CEO since 2005. Before joining the company, he served as Executive Vice President and COO for H&R Block, Inc.

ROBERT W HAU. He has served as the company's CFO since 2016. Before joining the company, he served as Executive Vice President and CFO at TE Connectivity Ltd. from 2012 to 2016. From 2009 to 2012, he served as Executive Vice President and CFO at Lennox International Inc.

LYNN S MCCREARY. She has served as the company's Chief Legal Officer (CLO) and Secretary since 2013. She joined the company in 2010 as Senior Vice President and Deputy General Counsel. Prior to joining the company, she was an attorney with the law firm of Bryan Cave LLP.

BYRON VIELEHR. He was promoted as the Chief Administrative Officer of the company in March 2018. He has served as the Group President, Depository Institution Services Group, from 2013 to 2018. Prior to joining Fiserv, he served in a succession of senior executive positions with The Dun & Bradstreet Corporation, from 2005 to 2013, most recently as the President of International and Global Operations.

ALISON DAVIS. Director since 2014. She is an advisor to Fifth Era and previously served as its Managing Partner from 2011 to 2015.

HARRY F DISIMONE. He was appointed as the company's director effective on February 21, 2018.

JOHN Y KIM. Director since 2016. He has served as President of New York Life Insurance Company since 2015.

DENNIS F LYNCH. Director since 2012. He is Chairman of Cardtronics plc. He was appointed Chairman in 2010 and has served as a director of Cardtronics since 2008.

DENIS J OLEARY. Director since 2008. He is a private investor.

KIM M ROBAK. Director since 2003. He has been a partner at Mueller Robak, LLC since 2004.

JD SHERMAN. Director since 2015. He has served as COO of HubSpot, Inc. since 2012 and as its President since 2014.

DOYLE R SIMONS. Director since 2007. He is President and CEO of Weyerhaeuser Company.

JOINT VENTURE

The company owns a 49% interest in StoneRiver Group, L.P. (StoneRiver), which is accounted for as an equity

method investment, and reports its share of StoneRiver's net income as income from investment in unconsolidated affiliate.

BUSINESS REGISTRATION

'ORATE AND BUSINESS REGISTRATIONS REPORTED BY THE SECRETARY OF STATE OR OTHER OFFICIAL SOURCE AS OF MAR 25 2019:

Registered Name: FISERV, INC.

Business type:	CORPORATION
Corporation type:	PROFIT
Date incorporated:	FEB 19 1992
State of incorporation:	WISCONSIN
Filing date:	FEB 19 1992
Registration ID:	F 024977
Status:	RESTORED TO GOOD STANDING
Status attained:	FEB 07 1996
Where filed:	SECRETARY OF STATE, MADISON, WI
Registered agent:	CORPORATION SERVICE COMPANY, 8040 EXCELSIOR DR;STE 400, MADISON, WI, 53717-291

OPERATIONS

12/27/2018

Description: The company, together with its subsidiaries, provides financial services technology. The company's Payments and Industry Products segment provides debit and credit card processing and services; electronic bill payment and presentment services; Internet and mobile banking software and services; person-to-person payment services; and other electronic payments software and services. This segment also offers card and print personalization services; investment account processing services for separately managed accounts; and fraud and risk management products and services.

Its Financial Institution Services segment provides account processing services, item processing and source capture services, loan origination and servicing products, cash management and consulting services and other products and services that support various types of financial transactions. This segment also offers a range of services, such as customization, business process outsourcing, education, consulting and implementation services; and ACH, treasury management, source capture optimization and enterprise cash and content management solutions, as well as case management and resolution services to the financial services industry.

The company also provides document and payment card production and distribution, check processing and imaging, source capture systems and lending and risk management products and services.

Terms are on contract basis. Sells to commercial concerns. Territory : International.

Nonseasonal.

Employees: 24,000 which includes officer(s). 65 employed here.

Facilities: Occupies premises in a building.

Branches: The business has branch(es) division(s); detailed branch information is available in Dun & Bradstreet's linkage or family tree products.

Subsidiaries: The business has subsidiary(ies); detailed subsidiary information is available in Dun & Bradstreet's linkage or family tree products.

FAMILY LINKAGE

This business is at the head of its corporate family tree. It is not a subsidiary of any other business.

UNSPSC

UNSPSC (United Nations Standard Product and Services Code) is a globally accepted commodity (Product and Services) classification system. FISERV, INC. offers the following product(s) and service(s):

81110000 **Computer services**
81112002 **Data processing or preparation services**

NAICS

Beginning in 1997, the **Standard Industrial Classification** (SIC) was replaced by the **North American Industry Classification System** (NAICS). This six digit code is a major revision that not only provides for newer industries, but also reorganizes the categories on a production/process-oriented basis. This new, uniform, industry-wide classification system has been designed as the index for statistical reporting of all economic activities of the U.S., Canada, and Mexico.

518210 **Data Processing, Hosting, and Related Services**
541511 **Custom Computer Programming Services**

SIC

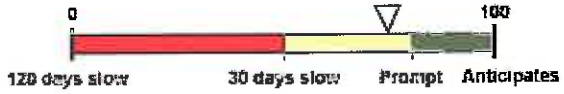
Based on information in our file, D&B has assigned this company an extended 8-digit SIC. D&B's use of 8-digit SICs enables us to be more specific to a company's operations than if we use the standard 4-digit code.

73749902 **Data processing service**
73710300 **Computer software development and applications**

D&B PAYDEX

The D&B PAYDEX is a unique, dollar weighted indicator of payment performance based on up to 192 payment experiences as reported to D&B by trade references.

3-Month D&B PAYDEX: 73
When weighted by dollar amount, payments to suppliers average 11 days beyond terms.



Based on trade collected over last 3 months.

D&B PAYDEX: 73
When weighted by dollar amount, payments to suppliers average 11 days beyond terms.



Based on up to 24 months of trade.
When dollar amounts are not considered, then approximately 69% of the company's payments are within terms.

PAYMENT SUMMARY

The Payment Summary section reflects payment information in D&B's file as of the date of this report.

Below is an overview of the company's dollar-weighted payments, segmented by its suppliers' primary industries:

	Total Rcv'd (#)	Total Dollar Amts ($)	Largest High Credit ($)	Within Terms (%)	Days Slow <31 (%)	31-60 (%)	61-90 (%)	90> (%)
Top industries:								
Whol computers/softwr	12	2,531,500	1,000,000	94	3	3	-	-
Prepackaged software	9	3,655,000	1,000,000	69	13	17	1	-
Telephone communictns	9	1,115,250	500,000	100	-	-	-	-
Nonclassified	8	1,466,000	900,000	97	3	-	-	-
Short-trm busn credit	7	630,000	400,000	88	4	4	4	-

Mfg computer storage	5	1,082,500	1,000,000	54	46	-	-	-
Mfg plane engine/part	5	750,000	400,000	18	77	-	5	-
Mfg misc office eqpt	3	1,700,000	1,000,000	79	9	12	-	-
Mfg computers	3	1,600,100	1,000,000	100	-	-	-	-
sanitary paper	1	750,000	750,000	100	-	-	-	-
OTHER INDUSTRIES	96	3,525,200	500,000	70	12	13	2	3
Other payment categories:								
Cash experiences	31	4,200	1,000					
Payment record unknown	2	100	50					
Unfavorable comments	0	0	0					
Placed for collections:								
With D&B	0	0						
Other	1	N/A						
Total in D&B's file	192	18,809,850	1,000,000					

The highest **Now Owes** on file is $1,000,000

The highest **Past Due** on file is $400,000

Dun & Bradstreet has 192 payment experiences in its file for this company. For your convenience, we have displayed 80 representative experiences in the PAYMENTS section.

PAYMENT DETAILS

Detailed payment history

Date Reported (mm/yy)	Paying Record	High Credit ($)	Now Owes ($)	Past Due ($)	Selling Terms	Last Sale Within (months)
03/19	Ppt		50	0		1 mo
	Ppt		50	0		1 mo
	Ppt		50	0		1 mo
	Ppt		50	0		1 mo
	Ppt	1,000,000	800,000	0		1 mo
	Ppt	1,000,000	1,000,000	0	N30	1 mo
	Ppt	900,000	0	0		4-5 mos
	Ppt	600,000	0	0		1 mo
	Ppt	400,000	0	0		4-5 mos
	Ppt	400,000	0	0		2-3 mos
	Ppt	250,000	200,000	0	PROX	1 mo
	Ppt	200,000	0	0		1 mo
	Ppt	100,000	50,000	0		1 mo
	Ppt	100,000	70,000	0		1 mo
	Ppt	35,000	10,000	750	Lease Agreemnt	1 mo
	Ppt	10,000	0	0		4-5 mos
	Ppt	7,500	2,500	0	N30	1 mo
	Ppt	5,000	2,500			2-3 mos
	Ppt	2,500	500	0		1 mo
	Ppt	1,000	0	0		6-12 mos
	Ppt	750	750	0		1 mo
	Ppt	750	0	0	N30	4-5 mos
	Ppt	500	0	0	N30	2-3 mos
	Ppt	250	0	0	N30	6-12 mos

	Ppt	250	250	0		1 mo
	Ppt	100	100	0		1 mo
	Ppt-Slow 30	40,000	0			1 mo
	Ppt-Slow 30	30,000	1,000	250		1 mo
	Ppt-Slow 30	15,000	0	0		1 mo
	Ppt-Slow 30	7,500	0	0		6-12 mos
	Ppt-Slow 30	2,500	2,500	1,000	Lease Agreemnt	1 mo
	Ppt-Slow 30	1,000	1,000	1,000	N30	1 mo
	Ppt-Slow 60	500,000	400,000	200,000		1 mo
	Ppt-Slow 60	10,000	0	0		4-5 mos
	Ppt-Slow 60	1,000	250	100	N30	1 mo
	Ppt-Slow 120+	30,000	0	0		6-12 mos
	Ppt-Slow 150	45,000	5,000			1 mo
	Slow 30	65,000	0			6-12 mos
	Slow 30	1,000	0	0		2-3 mos
	Slow 60	50	0	0		6-12 mos
	Slow 90	60,000	500	0		1 mo
	Slow 140	250	250	50		1 mo
	(043)	0	0	0	Cash account	6-12 mos
	(044)	0	0	0	Cash account	1 mo
02/19	Ppt	55,000	55,000	0		1 mo
	Ppt	40,000	0	0		6-12 mos
	Ppt	30,000	1,000	1,000		1 mo
	Ppt	20,000	0	0		2-3 mos
	Ppt	7,500	0	0		1 mo
	Ppt	7,500	0	0		4-5 mos
	Ppt	5,000	5,000	0		1 mo
	Ppt	2,500	2,500	0		1 mo
	Ppt	2,500	1,000	100		1 mo
	Ppt	250	0	0		6-12 mos
	Ppt	100	0	0	N30	6-12 mos
	Ppt	100	0	0		6-12 mos
	Ppt-Slow 30	1,000,000	1,000,000	400,000		1 mo
	Ppt-Slow 30	300,000	300,000	200,000		1 mo
	Ppt-Slow 30	100,000	100,000	45,000		1 mo
	Ppt-Slow 30	100,000	30,000	0		1 mo
	Ppt-Slow 30	75,000	75,000	20,000		1 mo
	Ppt-Slow 60	70,000	70,000	45,000		1 mo
	Slow 30	20,000	0	0		2-3 mos
	Slow 60	5,000	5,000	5,000		2-3 mos
	Slow 30-90	5,000	0	0		6-12 mos
	Slow 30-90+	500	0	0		4-5 mos
01/19	Ppt	5,000	0	0		6-12 mos
	Ppt	100	0	0	N30	6-12 mos
	Ppt	0	0	0		1 mo
	Ppt	0	0	0		1 mo
12/18	Ppt	1,000	0	0		6-12 mos
10/18	Ppt	15,000	15,000	0		1 mo
09/18	Ppt	500	0	0		6-12 mos
	Slow 240	2,500	2,500	2,500		
08/18	Ppt	2,500	2,500	0	N30	1 mo
	Slow 90+	2,500	0	0		6-12 mos
06/18	(077)				Sales COD	1 mo
05/18	Ppt	1,000	0	0		6-12 mos

04/18	Ppt	2,500			1 mo
03/18	Ppt-Slow 90	65,000	0	0	2-3 mos

Payment experiences reflect how bills are met in relation to the terms granted. In some instances payment beyond terms can be the result of disputes over merchandise, skipped invoices etc.

experience shown is from a separate supplier. Updated trade experiences replace those previously reported.

MENT TRENDS

SUPPLIER VERSUS INDUSTRY PAYDEX

->	PRIOR 4 QTRS				CURRENT 12 MONTH TREND											
	2017	---	---	2018	---	---	---	---	---	---	---	---	2019	---	---	---
	JUN	SEP	DEC	MAR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB	MAR	APR
Supplier PAYDEX	73	72	71	74	74	74	74	74	74	74	74	74	75	75	76	73
Industry PAYDEX (Based on 13 establishments in SIC 7374)																
UP QRT	80	80	80	80		80			80			80			80	
MEDIAN	77	78	77	77		78			77			77			77	
LO QRT	71	70	70	69		71			69			72			71	

PAYDEX scores are updated daily and are based on upto 24 months of trade experiences from the Dun& Bradstreet trade file.

All amounts displayed within this report are in local currency.

TEMENT UPDATE

02/22/2019

Fiscal Consolidated statement dated DEC 31 2018 (in thousands):

Assets		Liabilities	
Cash	415,000	Accts Pay	1,626,000
Accts Rec	1,049,000	Contract Liabilities	380,000
Prepaid Exps & Other Current Assets	760,000	L.T. Liab-(1yr)	4,000
Curr Assets	**2,224,000**	**Curr Liabs**	**2,010,000**
Fixt & Equip	398,000	Long-Term Debt	5,955,000
Intangible Assets-Net	2,143,000	Contract Liabilities	89,000
Goodwill	5,702,000	L.T. Liab-Other	915,000
Contract Costs-Net	419,000	COMMON STOCK	8,000
Other Assets	376,000	ADDIT. PD.-IN CAP	1,057,000
		ACCUM OTHER COMPREHENSIVE LOSS	(67,000)
		RETAINED EARNINGS	11,635,000
		TREASURY STOCK	(10,340,000)
Total Assets	**11,262,000**	**Total**	**11,262,000**

JAN 01 2018 to DEC 31 2018 annual sales $5,823,000,000; cost of goods sold $3,069,000,000. Gross profit [illegible]54,000,000; operating expenses $1,001,000,000. Operating income $1,753,000,000; other income $19,000,000; other expenses $207,000,000; net income before taxes $1,565,000,000; Federal income tax $378,000,000; net income $1,187,000,000.

Statement obtained from Securities And Exchange Commission. Prepared from statement(s) by Accountant: Deloitte &

Touche LLP, Milwaukee, Wisconsin.

ACCOUNTANT'S OPINION
"A review of the accountant's opinion indicated that the financial statement meets generally accepted accounting principles and the audit contains no qualifications.".

Fixed assets shown net less $829,000,000 depreciation.

Explanations
The net worth of this company includes intangibles; Other Long Term Liabilities consist of deferred income taxes and other long-term liabilities.

FINANCE

03/02/2018

Three-year statement comparative:

	Fiscal Consolidated Dec 31 2015 (000s omitted)	Fiscal Consolidated Dec 31 2016 (000s omitted)	Fiscal Consolidated Dec 31 2017 (000s omitted)
Current Assets	1,506,000	1,728,000	1,975,000
Current Liabs	1,502,000	1,820,000	1,938,000
Current Ratio	1.0	0.95	1.02
Working Capital	4,000	(92,000)	37,000
Other Assets	7,834,000	8,015,000	8,314,000
Net Worth	2,660,000	2,541,000	2,731,000
Sales	5,254,000	5,505,000	5,696,000
Long Term Liab	5,178,000	5,382,000	5,620,000
Net Profit (Loss)	712,000	930,000	1,246,000

Fiscal Consolidated statement dated DEC 31 2017:

Assets		Liabilities	
Cash	325,000	Accts Payable & Other Accrued Exps	1,383,000
Accts Rec	997,000	Curr Maturities of L.T. Debt	3,000
Prepaid Exps & Other Curr Assets	603,000	Deferred Revenue	552,000
Assets Held for Sale	50,000		
Curr Assets	**1,975,000**	**Curr Liabs**	**1,938,000**
Fixt & Equip	390,000	Long-Term Debt	4,897,000
Intangible Assets-Net	1,882,000	Deferred Income Taxes	552,000
Goodwill	5,590,000	L.T. Liab-Other	171,000
Other Long-Term Assets	452,000	COMMON STOCK	4,000
		ADDIT. PD.-IN CAP	1,035,000
		ACCUM OTHER COMPREHENSIVE LOSS	(54,000)
		RETAINED EARNINGS	10,240,000
		TREASURY STOCK	(8,494,000)
Total Assets	**10,289,000**	**Total**	**10,289,000**

From JAN 01 2017 to DEC 31 2017 annual sales $5,696,000,000; cost of goods sold $3,024,000,000. Gross profit $2,672,000,000; operating expenses $1,140,000,000. Operating income $1,532,000,000; other income $2,000,000; other expenses $176,000,000; net income before taxes $1,358,000,000; Federal income tax $158,000,000. Net income $1,246,000,000. Income from Investment $32,000,000. Income from Disc Oprs $14,000,000.

Prepared from statement(s) by Accountant: Deloitte & Touche LLP, Milwaukee, WI.

ACCOUNTANT'S OPINION
A review of the accountant's opinion indicates the financial statements meet generally accepted accounting principles and that the audit contains no qualifications.

Explanation
The networth of this company includes intangibles.

The report was updated using information the company filed with the Securities and Exchange Commission.

BUSINESS RATIOS

Statement date: DEC 31 2018
Based on this number of establishments: 13

Firm		Industry Median		Quartile Rank (Supplier)
Return of Sales:	20.4	Return of Sales:	7.6	1
Current Ratio:	1.1	Current Ratio:	1.6	3
Quick Ratio:	0.7	Quick Ratio:	1.3	4
Assets / Sales:	193.4	Assets / Sales:	155.5	3
Total Liability / Net Worth:	391.1	Total Liability / Net Worth:	185.2	4

PUBLIC FILINGS

The following Public Filing data is for information purposes only and is not the official record. Certified copies can only be obtained from the official source.

SUITS

Status: **Pending**
CASE NO.: 2019CV000376
Plaintiff: GARFIELD, ROBERT, ENGLEWOOD, FL
Defendant: FISERV, INC. AND OTHERS
Cause: INTERNAL BUSINESS ORGANIZATIONAL CLAIMS
Where filed: WAUKESHA COUNTY CIRCUIT COURT, WAUKESHA, WI

Date status attained: 02/28/2019
Date filed: 02/28/2019
Latest Info Received: 03/14/2019

Status: **Pending**
CASE NO.: 2018-002504-2
Plaintiff: HOSTETLER, JOHN
Defendant: FISERV, INC. AND OTHERS
Cause: CONTRACT - DEBT/CONTRACT - FRAUD/MISREPRESENTATION
Where filed: TARRANT COUNTY - COUNTY AT LAW COURT, FORT WORTH, TX

Date status attained: 04/26/2018
Date filed: 04/26/2018
Latest Info Received: 05/31/2018

Status: **Judgment entered**
CASE NO.: 201800004898SCSCCTL
Plaintiff: KEILHOLTZ, ROBERT G
Defendant: FISERV INC
Cause: SMALL CLAIMS
Where filed: SAN DIEGO COUNTY SMALL CLAIMS COURT/SAN DIEGO, SAN DIEGO, CA

Date status attained: 11/08/2018
Date filed: 01/30/2018
Latest Info Received: 02/06/2019

Status: **Pending**
CASE NO.: INS1501872
Plaintiff: RICHARD HOPE
Defendant: FISERV AND OTHERS
Cause: SMALL CLAIMS-OVER $1500/UNDER $5000
Where filed: RIVERSIDE COUNTY SMALL CLAIMS COURT/INDIO, INDIO, CA

Date status attained: 10/30/2015
Date filed: 10/30/2015

Latest Info Received: 11/12/2015

Status: **Pending**
CASE NO.: 017-276927-15
Plaintiff: MAC CHURCHILL ACURA MAC CHURCHILL, INC.
Defendant: FISERV, INC. AND OTHERS
Cause: OTHER
Where filed: TARRANT COUNTY CIVIL DISTRICT COURT, FORT WORTH, TX

Date status attained: 02/17/2015
Date filed: 02/17/2015
Latest Info Received: 03/12/2015

If it is indicated that there are defendants other than the report subject, the lawsuit may be an action to clear title to property and does not necessarily imply a claim for money against the subject.
There are additional Suits in D&B's file on this company available by contacting 1-800-234-3867.

LIENS

A lienholder can file the same lien in more than one filing location. The appearance of multiple liens filed by the same lienholder against a debtor may be indicative of such an occurrence.

Amount: **$14,737**
Status: **Open**
DOCKET/WARRANT: X071833
Type: State Tax
Filed by: NYS TAX COMMISSION
Against: AFTECH, MALVERN, PA AND OTHERS
Where filed: ALBANY COUNTY SUPREME COURT, ALBANY, NY

Date status attained: 01/19/2007
Date filed: 01/19/2007
Latest Info Received: 04/12/2007

UCC FILINGS

Collateral: Negotiable instruments - Inventory - Account(s) - Oil, gas and minerals - and OTHERS
Type: Original
Sec. party: STATE BANK OF HERSCHER, HERSCHER, IL
Debtor: KRIPPEL, DENNIS E, PONTIAC, IL
Filing number: 020195630
Filed with: SECRETARY OF STATE/UCC DIVISION, SPRINGFIELD, IL

Date filed: 04/06/2015
Latest Info Received: 04/17/2015

Type: Termination
Sec. party: STATE BANK OF HERSCHER, HERSCHER, IL
Debtor: KRIPPEL, DENNIS E, PONTIAC, IL
Filing number: 002026350
Filed with: SECRETARY OF STATE/UCC DIVISION, SPRINGFIELD, IL

Date filed: 04/13/2018
Latest Info Received: 04/15/2018
Original UCC filed date: 04/06/2015
Original filing no.: 020195630

Collateral: Account(s) and proceeds - General intangibles(s) and proceeds - Leased Computer equipment and proceeds - Leased Equipment and proceeds
Type: Original
Sec. party: PNC EQUIPMENT FINANCE, LLC, CINCINNATI, OH
Debtor: FISERV INC. and OTHERS
Filing number: 130016664023
Filed with: SECRETARY OF STATE/UCC DIVISION, MADISON, WI

Date filed: 12/30/2013
Latest Info Received: 01/22/2014

Type: Amendment
Sec. party: PNC EQUIPMENT FINANCE, LLC, CINCINNATI, OH

Debtor: FISERV INC. and OTHERS
Filing number: 130016777533
Filed with: SECRETARY OF STATE/UCC DIVISION, MADISON, WI

Date filed: 12/31/2013
Latest Info Received: 01/22/2014
Original UCC filed date: 12/30/2013
Original filing no.: 130016664023

Type: Continuation
Sec. party: PNC EQUIPMENT FINANCE, LLC, CINCINNATI, OH
Debtor: FISERV INC. and OTHERS
Filing number: 180010649626
Filed with: SECRETARY OF STATE/UCC DIVISION, MADISON, WI

Date filed: 08/02/2018
Latest Info Received: 09/07/2018
Original UCC filed date: 12/30/2013
Original filing no.: 130016664023

There are additional UCC's in D&B's file on this company available by contacting 1-800-234-3867.

The public record items contained in this report may have been paid, terminated, vacated or released prior to the date this report was printed.

GOVERNMENT ACTIVITY

Activity summary

Borrower (Dir/Guar):	NO
Administrative debt:	NO
Contractor:	YES
Grantee:	NO
Party excluded from federal program(s):	NO
Congressional District:	05

details provided in the Government Activity section are as reported to Dun & Bradstreet by the federal rnment and other sources.

Copyright 2019 Dun & Bradstreet - Provided under contract for the exclusive use of subscriber 263159923

3.0 Attachment 4: Project Organization and Staffing Approach

RFP Section 5.4.2.10 (Table 11) & Attachment 4, pp. 74 & 110

1. Instructions

Staffing strategies are to be employed by the Vendor to ensure all requirements and service levels are met to the satisfaction of the Department of Health and Human Resources (DHHR).

1.1 The evaluation of the Vendor's staffing approach shall be based on the ability of the Vendor to satisfy the requirements stated herein. Therefore, the Vendor should present detailed information regarding the expertise of the proposed staff and an Initial Staffing Plan.

1.2 For ease of formatting and evaluation Attachment 4: Project Organization and Staffing Approach Provides the required outline for the Vendor's response to staffing.

1.2.1 The Vendor's response to the following should not exceed 25 pages, excluding key personnel resumes and the forms provided in this Attachment.

1.2.2 Refer to request for proposal (RFP) Section 4.7.1 Qualifications and Experience for the details pertaining to staff qualifications, experience, and responsibilities.

FDGS offers a unique combination of EVV experts, business process acumen and CMS programmatic subject matter expertise to validate that our EVV solution fits within the appropriate context of business needs, financial constraints, and client services for WV DHHR and its beneficiaries.

For your contract, FDGS will assemble a team that provides the practical knowledge, experience, and expertise required for the design, implementation, and operations of your EVV solution. This includes methodologies, tools, and best practices acquired over the years from multiple statewide EVV projects. This minimizes the risk to the Department's ongoing services while AuthentiCare is deployed to providers and beneficiaries throughout West Virginia.

2. Initial Staffing Plan

2.1 As part of the Vendor's bid response, the Vendor should provide an Initial Staffing Plan. In addition to the requirements described in Appendix 1:Detailed Specifications , the Vendor's narrative description of its proposed Initial Staffing Plan should include the following:

2.1.1 A succinct description of the Vendor's proposed project team and should exhibit the Vendor's ability and capability to provide knowledgeable, skilled, and experienced personnel to accomplish the Scope of Work (SOW) as described in this RFP.

2.1.2 A detailed proposal for providing all resources necessary to fulfill the requirements as specified in this RFP. This includes details covering both key and support staff.

2.1.3 Organization charts for implementation and maintenance stages showing both the Vendor staff and their relationship to DHHR staff that will be required to support the project. The organization chart should denote all key staff for this project, and a summary of each key member's high-level responsibilities.

2.1.4 A narrative describing tools and processes used to screen available staff to fill positions. In addition, a narrative describing the process for replacing key staff within defined timeframes and procedures for backfilling key staff during any transition.

2.1.5 Resumes (maximum two pages each) for the key staff and any additional staff members the Vendor will have assigned to this project including their licenses, credentials, and experience. DHHR considers the key staff resumes as a key indicator of the Vendor's understanding of the skill sets required for each staffing area.

2.1.6 A letter of intent for each proposed staff member not currently employed by the Vendor. Each letter of intent should be signed by the named individual, indicating that the individual is willing to accept employment if the Vendor is awarded the contract.

2.1.7 A description and organizational diagram of the proposed staffing for each phase of the project.

2.1.8 Identification of subcontractor staff, if applicable.

3.1 Initial Staffing Plan

FDGS provides a team of professionals with industry, technology, and AuthentiCare experience who collectively deliver success for WV. The staffing approach that FDGS uses is to hire great people and provide them with the tools and leadership they need to succeed.

Our initial staff management plan provides the framework for staff resource estimating, staff ramp-up, and resource loading for all phases of the implementation periods. The staff management plan also includes the ramp down of staffing during the transition to Maintenance and Operations (M&O), and aligns with the standards of PMI and its PMBOK® guide. During the initiation phase of the project, our EVV project leaders verify and validate the plan for all necessary staff needed to complete the scope of work throughout the duration of the project.

The project schedule is decomposed into several phases. We make high-level staffing estimates and a schedule of phases. To validate these high-level estimates, we create a work breakdown structure. The decomposition continues until the tasks or work units reach a level where they can be accurately defined and estimated. This becomes the basis for dividing work into definable increments, and technical, schedule, and staffing requirements can be established.

We consider factors like specific skill sets, experience of staff at similar projects, successes of specific staff, and team experience when determining how and where to acquire staff. Additional factors include the complexity and size of the project, the need for specialized knowledge, and integration experience.

FDGS has almost two decades of experience with EVV, and a strong resource pool of specialists, which provides the ability to maintain the staffing levels needed for successful project outcomes. The Project Manager evaluates the schedule weekly to confirm that the project remains on track. If the project starts to drift, there are techniques that we can use to get back on schedule, including:

- **Fast Tracking:** Fast tracking looks at activities on the critical path that are normally done in sequence and assigns them in parallel. This may not require additional staff.
- **Schedule Crashing:** "Crashing" the schedule means focusing additional resources to the critical path. Crashing generally involves bringing additional resources in for a fixed period of time.

FDGS agrees to provide and maintain staffing levels to complete the implementation of our AuthentiCare EVV solution according to the approved project schedule. The Project Manager will prepare a project plan for modifications or enhancements requested by DHHR. This plan will contain an estimate of staff effort and task schedule, including impact on other project activities and priorities, and submitted for approval to proceed.

Staff Capabilities and Experience

Our initial staffing plan is built on a record of accomplishment performing the work required to realize similar specific goals and objectives, with a specific focus on compliance with the 21st Century Cures Act by the end of the year and CMS certification soon after.

Our commitment to quality starts at the top. FDGS brings an experienced management team with a comprehensive understanding of systems and solutions specific to Medicaid EVV

programs. This experience enables our team to bring solutions, implementation strategies, and best practices from some of the latest projects in the country, including the knowledge, experience, and lessons learned from other AuthentiCare implementations. The key personnel proposed for the West Virginia EVV project meet or exceed the minimum qualifications for their respective roles and have successfully deployed AuthentiCare in other states. Table 3.1 lists our key personnel and the team supporting the WV DHHR EVV project.

Table 3.1 – Key and Supporting Personnel for West Virginia's EVV Project

Role	Resource
Executive Oversight	King Farias
Account Manager – Key	Asad Salahuddin
Project Manager – Key	David Sullivan
Quality Manager – Key	Cayle Cox
Technical/Development Leads	Pool of skilled resources
Product Specialists	Pool of skilled resources
Senior Business Analysts	Pool of skilled resources
Testing Specialists	Testing Center of Excellence Pool of skilled resources
CMS Certification SMEs	Pool of skilled resources
Training Manager	TBD
Support/Operations Specialist	Pool of skilled resources

Figure 3.1 illustrates the organizational structure of our proposed AuthentiCare Team, highlighting key staff scheduled during the implementation period of the West Virginia EVV project.

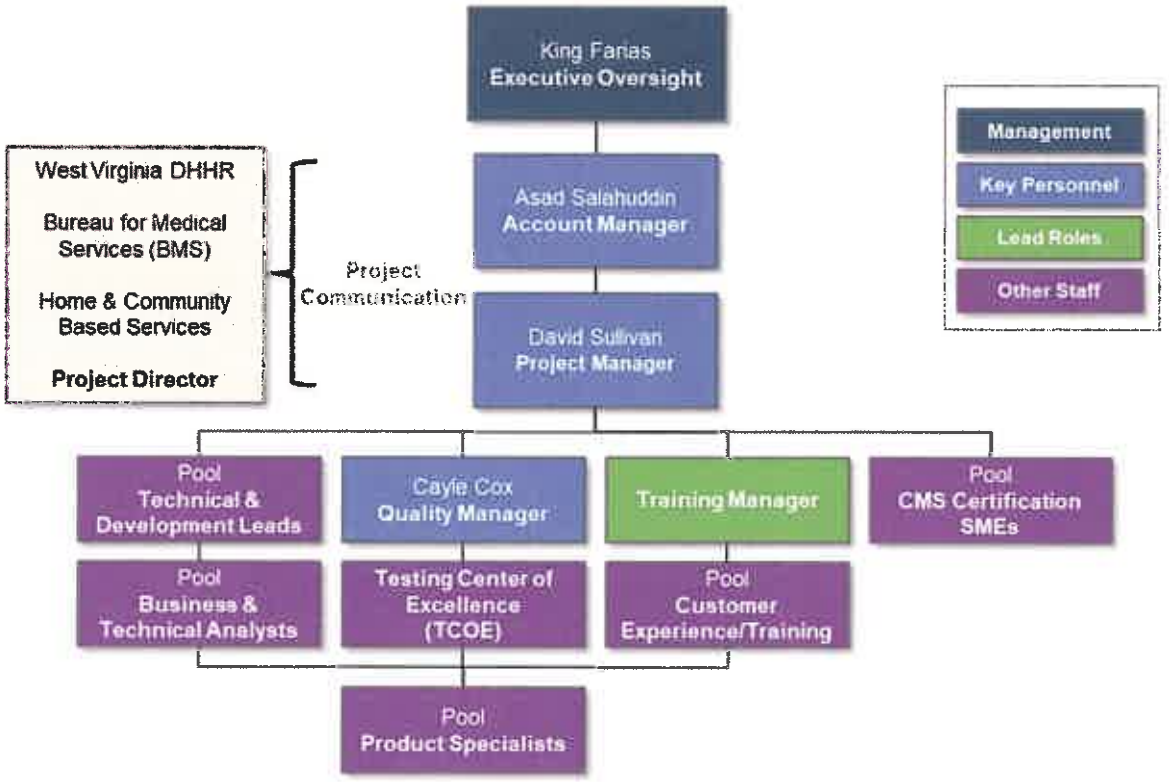


Figure 3.1 – FDGS Project Implementation Organizational Chart for West Virginia's EVV

DHHR needs an experienced and reliable vendor to lead the EVV project. FDGS has assembled a team of experienced staff to successfully implement the program and provide consistent, ongoing operation of the EVV components throughout the duration of the contract.

Our staff selection processes are deliberate and comprehensive. They are based on each team member's proven ability to accomplish the scope of work efficiently, effectively, and with quality results. Our proposed team includes Management, Supervisory, Key Personnel, and a list of AuthentiCare product support staff.

The FDGS Project Manager will be the main point of contact for DHHR staff. For some executive meetings and any topics that require escalation, our Project Manager will make sure to include the FDGS Account Manager as needed.

We have examined the organizational charts provided in the RFP for DHHR and the Bureau for Medical Services (BMS) and the Office of Management Information Services (OMIS). Upon award, we will work with the Department to identify the corresponding points of contact at both BMS and OMIS to support the EVV project and maintain clear lines of communication. We assume that a Project Director or similar role will be assigned to the EVV project as the primary contact for our Project Manager. For technical topics, including system interfaces and integration with the MMIS, FDGS will also name a Technical Lead to work with the assigned EVV technical lead from OMIS.

Staffing Transition between Implementation and Operations

FDGS will transition oversight of the WV EVV system to our Account Manager and Operations Manager for the day-to-day operation of the system. The Account Manager will be responsible

for project communication with the WV DHHR Project Director. Once we are in the Operations Phase, the Account Manager has increased communication responsibilities with WV DHHR for any necessary escalations. Additionally, the Account Manager now works directly with the Operations Manager who oversees all operations and support activities with modified resource pools.

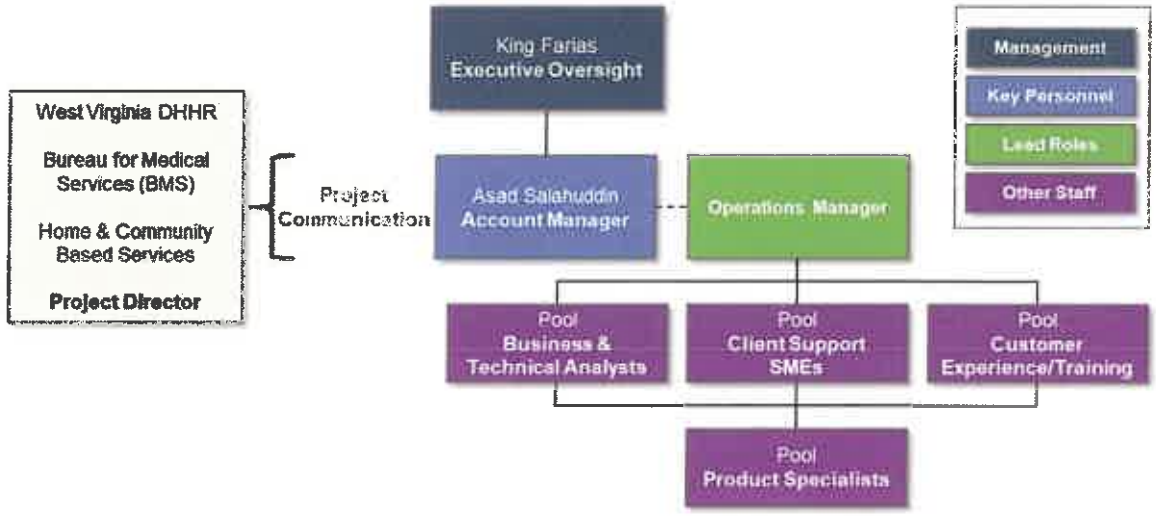


Figure 3.2 – FDGS Project Operations Organizational Chart for West Virginia's EVV

Staffing Levels and Staffing Approach

Staff turnover is kept to a minimum to the extent possible. However, if a departure from the project is unavoidable, FDGS will put in place qualified backup staff with comparable skills and experience to maintain agreed-upon delivery and operational targets.

The Project Manager monitors the project plans and risk register to anticipate potential changes in staffing needs and works closely with the FDGS dedicated Resource Manager to address them. The FDGS Resource Manager continuously reviews our staff resource pool for staff who have the skills and qualifications, as well as the "cultural fit" to integrate well into a project. As standard practice, corporate resources approaching the conclusion of assignments are actively monitored, screened and proactively discussed with our project managers to understand where staff changes and staff availability align.

To build and maintain our pool of experienced resources, our Resource Manager uses tools including an updated candidate database, skills matrix by program, and referral programs. Beyond our corporate resource pool, the Resource Manager continuously recruits and screens top talent to join our organization. Having an additional network of talented resources at our fingertips, already pre-screened and interested in joining our organization, further enables us to respond quickly as staffing needs arise.

When addressing a staff change, the Project Manager (or designee) and Resource Manager review our internal resource pool against the position description to quickly identify the right replacement resource. Our selection process considers the position requirements as well as the project culture to identify the right resource to quickly integrate with the established team. Whether a resource is requested off the project, or an unplanned staffing change occurs, FDGS agrees to immediately communicate with DHHR to define an interim plan and initiate our

processes to identify replacement staff. Once a resource has been selected for replacement, the Project Manager or designee will notify the Department and provide resumes for approval. Replacement resources will not begin work on the project until DHHR approves them.

FDGS does not propose the use of subcontractors at this time. If subcontractors are required in the future phases of the contract, we will work with the Department to follow the required procurement rules for subcontractors to be properly added to the contract.

We provide an overview of the key and supporting personnel below. The entire team is knowledgeable in the AuthentiCare application and its processes, and understands the solution's importance to West Virginia, its providers, and its beneficiaries.

Table 3.2 – AuthentiCare Project Roles and Responsibilities

Role	Responsibilities
Executive Oversight	• Provide professional after-award support with focus on customer satisfaction • Remain in frequent contact with DHHR to understand project concerns and executive relationships • Respond to escalation points and resolve issues
Project Manager	The Project Manager is responsible for the execution and completion of the day-to-day project tasks. The Project Manager serves as the primary point of contact for all day-to-day technical and functional matters relating to the execution of the project: • Provide day-to-day management of West Virginia EVV Project and AuthentiCare delivery team • Review and monitor the Work Plan tasks, deliverables, and milestones to confirm that the project is on schedule • Interface with client daily • Direct the completion of project tasks within estimated time frames and budget constraints • Serve as a key contributor in preparing and reviewing project deliverables • Interface with project stakeholders including stakeholders from other related projects • Develop performance metrics and benchmarks • Administer communication between the AuthentiCare delivery team and all project stakeholders, including: ▪ Reporting key metrics, milestones, and policies and procedures ▪ Working with the State's Project Team to facilitate proper communication ▪ Communicating with stakeholders to streamline communication ▪ Confirming that dashboard reporting is provided to stakeholders ▪ Managing communications channels to deliver messages effectively • Establish and maintain controls to monitor budget and cost projections, resource allocations, and time reporting • Provide timely completion of all FDGS deliverables and work products
Account Manager	The Account Manager represents and oversees all contractual aspects of the project, and is authorized to negotiate contract terms and conditions including: • Serving as the single point of contact for all day-to-day contractual matters relating to the execution of the project contract • Maintaining contractual records and documentation like receipt and control of all contract correspondence, customer contact information sheets, contractual changes, status reports and other documents • Providing guidance on contract matters to the Project Manager, Operations Manager, or other project and operational staff as needed • Handle ongoing issue and change management • Monitor transaction compliance (milestones, deliverables, invoicing, etc.)
Operations Manager	The Operations Manager is responsible for day-to-day operations of the AuthentiCare platform for DHHR. The Operations Manager leads the operational status meetings

Role	Responsibilities
	with WV staff, and FDGS staff, and works with WV DHHR to prioritize activities for the operations team. The Operations Manager will: • Collaborate with the project team to stay involved in the planning efforts for new releases and production interaction • Manage meetings including the presentation of an agenda, facilitation of the call, and capture of meeting minutes • Offer to host provider forums via online or call-in formats along with the Operations Analyst and the AuthentiCare Product team, • Work closely with our Global Infrastructure Operations (GIO) Capacity Management team to monitor the AuthentiCare platform capacity statistics and plan recommended improvements on a quarterly basis, if needed. • Track ongoing feedback in the project issues tracking document. After the issues have been identified, the Operations Manager will work with the various teams to determine who has ownership of the issues and track the status and resolution of the issue.
Quality Manager	The Quality Manager will: • Devise procedures to inspect and report on quality issues • Monitor all operations that affect quality • Supervise and guide inspectors, technicians, and other staff • Verify the reliability and consistency of production by checking processes and final output • Appraise client requirements and confirm that work meets client standards • Facilitate proactive solutions by collecting and analyzing quality data • Review current standards and policies • Keep records of quality reports, statistical reviews, and relevant documentation
Training Manager	The Training Manager is responsible for planning all project training efforts and implementing the Training plan. The Training Manager will: • Create the training schedule, content, presentations, and draft training materials • Lead webinars and other relevant trainings to Department staff, providers, MCOs, and other end users • Review call center dashboards to identify training opportunities • Create catered training materials for varied stakeholders and users of the AuthentiCare solution. • Engage during project implementation phase and continue to provide support on project enhancements and release rollouts to minimize issues.
Business and Technical Analyst Pool	FDGS maintains a pool of highly skilled Senior Business and Technical Analysts who specialize in the development, delivery, and implementation of EVV projects. These analysts: • Provide support and assistance to projects • Review and prepare deliverables • Evaluate and analyze risk • Provide quality assurance and training support to the on-the-ground
Product Specialist Pool	FDGS maintains a pool of Product Specialists that support the AuthentiCare EVV product. These specialists: • Function as experts on AuthentiCare features, functions, and infrastructure • Monitor federal and state requirements and requests for new features and EVV capabilities • Provide support for defect troubleshooting, root cause analysis, and problem resolution
Certification SME Pool	The Certification SME pool will support AuthentiCare requirements definition and project activities from Project Initiation through to formal certification by CMS including: • Reviewing any applicable CMS updates to the Certification process • Participating in Requirements Validation and design/configuration sessions to identify requirements specific to CMS Certification • Working with Business Analyst and Test Analyst on scenarios for business function

Role	Responsibilities
	CMS requirements and test case development • Reviewing test cases and results for the CMS certification scenarios and validation • Supporting Training & Outreach in areas such as HIPAA awareness training materials in the various user role training • Identifying and support the gathering of all required evidence for CMS Certification
Technical and Development Leads Pool	FDGS maintains a pool of experienced senior application architect and technical resources to transform customer specifications into actual design and development of software systems. • Technical leads: ▪ Responsible for maintaining and evolving the AuthentiCare platform. Provide technical oversight and coordination of the EVV systems and integration, development, quality assurance, and testing ▪ Guide the lead developers who modify the AuthentiCare application based on approved product enhancements • Security leads safeguard and protect all user data and maintain compliance with data standards, rules, and regulations for all applicable data within the AuthentiCare system
Client Support SMEs Pool	Our tiered Client Support SMEs Pool confirms that the proper attention is given to the needs of the client. The Tier 1 Call Center Representatives are the first line of contact for providers to reset passwords, research claims, review authorizations, and create tickets.
Customer Experience/Training Pool	FDGS maintains a pool of AuthentiCare training and outreach specialists overseen by a Training Manager focused on customer outreach, as well as AuthentiCare's training and education program. These specialists: • Provide users a positive customer experience by delivering effective training • Maintain user guides and customer-facing documentation • Keep an open line of communication with all stakeholders, including State staff, Managed Care Organizations, program providers, and clients • Work with stakeholders in every phase of AuthentiCare's development life cycle, and continue its post-implementation engagement by supporting customers during the Maintenance and Operations (M&O) phase
Testing Center of Excellence (TCOE)	FDGS follows a disciplined Quality Assurance (QA) approach that contributes to our record of delivering projects on time, within budget, and with high quality. This Structured Test Methodology (STM) verifies that all functional and system-wide requirements are complete and confirms the configuration requirements. In support of the STM, FDGS has a dedicated team of testing subject matter experts that comprise our Testing Center of Excellence (TCOE). The TCOE is equipped with the processes, technology, tools, infrastructure, and talent to support quality deliverables. The project team works closely to engage TCOE resources according to the project work plan, providing the highest level of quality assurance throughout the entire lifecycle of the EVV project.

3.1.1 Pool Staff Supporting AuthentiCare

Technical/Development Leads Pool

FDGS maintains a pool of experienced senior application architect and technical resources to transform customer specifications into actual design and development of software systems. Our application development leaders have served as senior application architects for the AuthentiCare solution. Our technical leads are responsible for maintaining and evolving the AuthentiCare platform. Responsibilities include providing technical oversight and coordination of the EVV systems and integration, development, quality assurance, and testing. Technical Leads provide guidance for the lead developers who will modify the AuthentiCare application based on approved product enhancements. Our security leads maintain safeguarding and protection of all

user data and compliance with data standards, rules and regulations for all applicable data within the AuthentiCare system.

While we will assign a specific lead to the West Virginia EVV project, we also maintain an experienced technical team supporting AuthentiCare behind the scenes. Decades of experience exist in our technical team, which includes several other technical experts covering areas of the EVV solution including technical oversight and coordination, technical analysis and design, data architecture, and solution architecture.

Senior Business Analyst Pool

FDGS maintains a pool of highly skilled Senior Business Analysts who specialize in the development, delivery, and implementation of EVV projects. FDGS Business analysts are available to provide guidance, support and assistance to projects in any capacity from the review and preparation of deliverables, evaluation and analysis of risk, to quality assurance and training support for the on-the-ground staffing needed during kick-off and implementation processes. It is our established best practice to identify one or more specific business analysts, as defined in our proposals, to be dedicated to individual projects. Beyond assigning a dedicated Senior Business Analyst to the project, we will have a secondary resource stay engaged and informed via status meetings and regular interaction with the DHHR project team to easily engage if and when necessary, maintaining productivity levels and quality throughout.

Product Specialist Pool

FDGS maintains a pool of Product Specialists that support the AuthentiCare EVV product. Our Product Specialists are focused on the AuthentiCare features and functions, as well as the infrastructure supporting our multiple user interface platforms. The AuthentiCare Product Specialists provide a two-fold benefit to FDGS and our customers. First, our team continually monitors federal and state requirements and requests for new features and EVV capabilities. This feedback is the primary input to the AuthentiCare product roadmap for future enhancements that will be made available to all AuthentiCare customers. Second, the Product Specialists provide an additional level of support for defect troubleshooting, root cause analysis, and problem resolution.

Testing Specialists Pool (Testing Center of Excellence)

FDGS follows a disciplined Quality Assurance (QA) approach that contributes to our record of delivering projects on time, within budget, and with high quality. This Structured Test Methodology (STM) verifies that all functional and system-wide requirements are complete and confirms the configuration requirements.

In support of the STM, FDGS has a dedicated team of testing subject matter experts who comprise our Testing Center of Excellence (TCoE). The TCoE is equipped with the processes, technology, tools, infrastructure, and talent to support quality deliverables. The project team works closely to engage TCoE resources according to the project work plan, providing the highest level of quality assurance throughout the entire lifecycle of the EVV project.

Customer Experience and Training Pool

FDGS maintains a pool of Delivery Analysts overseen by a dedicated Customer Experience and Outreach Manager focused on customer outreach, as well as AuthentiCare's training and education program. Their priority is for AuthentiCare users to have a positive customer experience by delivering effective training, to maintain user guides and customer-facing documentation, and keep an open line of communication with all stakeholders, including State

staff, Managed Care Organizations, program providers, and clients. To maximize the Delivery Analysts' training capabilities, and to reach a geographically and culturally diverse audience, the training delivery methodologies include on-site sessions, real-time webinars, self-paced e-learning modules, and user guides. The team of Delivery Analysts works alongside stakeholders in every phase of AuthentiCare's development life cycle, and continues its post-implementation engagement by supporting customers during the Maintenance and Operations (M&O) phase.

CMS Certification Subject Matter Experts Pool

FDGS understands the certification guidance and requirements based on regular communication with CMS and our hands-on project experience (with points of view as both an EVV contractor and IV&V vendor for other states). Our SMEs are experts in Medicaid policy and are skilled in helping our clients maximize their federal funding matches.

Our CMS Certification SMEs are currently engaged in OBC planning of the CMS certification process with our customers the Division of Health Care Financing and Policy (DHCFP) for the State of Nevada, the Oklahoma Department of Human Services, and with Kansas Department of Aging and Disability Services. We have been working with the CMS Technical Director over CMS Certification nationally, and his team, to clarify and better define the OBC requirements and guidance since September 2019. Nevada's DHCFP will be one of the first agencies to use the new EVV OBC process for certification, with planned CMS Certification end of Q2 2020. With FDGS working across multiple customers using OBC for CMS certification to qualify for enhanced federal funding, we will bring extensive experience and knowledge to West Virginia for your successful CMS OBC certification approval.

FDGS provides a unique perspective on what is necessary to satisfy CMS mandates and state imperatives. The combination of our AuthentiCare solution with our CMS certification experience is unparalleled in the current marketplace.

Client Support SMEs Pool

Our tiered Client Support SMEs Pool confirms that the proper attention is given to the needs of the client. The Tier 1 Call Center Representatives are the first line of contact for providers to reset passwords, research claims, review authorizations, and create tickets.

Items that require advanced assistance or calls outside of the core hours are handled by the Tier 2 Help Desk Specialist Team. Tier 3 AuthentiCare Subject Matter Experts are experts from various departments who are available to Tier 1 and Tier 2 staff members as an escalation point on advanced issues. They provide advanced data research capabilities along with providing analytical analysis needed to review relationships and outcomes based on business rule and application code functionality. Tier 3 resources are assigned to issues when needed through a formal escalation process.

3.2 Key Staff, Resumes, and References

3. Key Staff, Resumes, and References
3.1 Key Staff
Key staff consist of the project's senior leadership for the Electronic Visit Verification (EVV) project. These resources are responsible for providing leadership, and creating the standards and processes required for the successful implementation, operation, maintenance.
3.1.1 The Vendor should make the proposed key staff available for an in-person interview upon DHHR's request.
3.1.2 To ensure successful transition to the operations phase, the implementation activities should be led by key staff identified in the list below :
3.1.2.1 Account Manager
3.1.2.2 Project Manager
3.1.2.3 Quality Assurance Manager
3.1.3 The qualifications, experience, and responsibilities for each key staff role are defined in RFP Section 4. 7.1 Qualifications and Experience: Table 8: Staff Qualifications, Experience, and Responsibilities.
3.2 Resumes
3.2.1 Resumes for key staff named in the Vendor proposal should indicate the role of the staff on the EVV project and demonstrate how each staff member's experience and education will contribute to the successful implementation of the EVV.
3.2.2 Each resume should demonstrate experience relevant to the position proposed. If applicable, resume should include work on projects cited under the Vendor's corporate experience, and the specific functions performed on such projects.
3.2.3 The Vendor should complete Table 23: Resumes for Proposed Key Staff and include in this section Proposed Key Staff resumes and any additional staff members' resumes the Vendor will have assigned to this project.
3.3 References
3.3.1 The Vendor should provide three (3) references for which each proposed key staff candidate has successfully demonstrated meeting the requirements of the RFP. The name of the person to be contacted, phone number, client name, address, brief description of work, and date (month and year) of employment should be given for each reference. These references should be able to attest to the candidate's specific qualifications.
3.3.2 The reference given should be a person within a client's organization and not a co-worker or a contact within the Vendor's organization.
3.3.3 Vendors should use the format provided in Table 24: Key Staff References. Repeat the rows and tables as necessary

The scope of this project requires three key staff from RFP Table 8: Staff Qualifications, Experience, and Responsibilities – Account Manager, Project Manager, and Quality Manager. As required, FDGS will make proposed key staff available for in-person interviews if requested by DHHR. Our proposed key staff for the West Virginia EVV project meet or exceed all qualifications noted in the RFP for each respective role. All proposed staff are already FDGS employees so the requested letters of intent are not applicable.

Key – Account Manager: Asad Salahuddin

Mr. Asad Salahuddin is an experienced Project Management Professional (PMP) and ITIL-certified Account and Contract Manager with specialized experience in AuthentiCare projects and systems management. He brings extensive EVV Subject Matter Expertise. He served as Account Manager for our New Mexico EVV project with four of the largest Managed Care Organizations (MCO) in the country. He is currently engaged as the Account Manager for the State of Oklahoma's EVV implementation. Mr. Salahuddin is skilled in handling the responsibilities associated with the development and delivery of large-scale EVV projects including providing primary support for the application, adherence to contractual SLAs related to system availability (Web, Mobile, and IVR), timely and accurate processing of electronic claims for payment file processing, reports availability, client issues, product enhancement, communications, and seamless onboarding procedures with the state staff, clients, and providers.

Key – Project Manager: David Sullivan

Mr. Sullivan is a Certified PMP and Certified Scrum Master with expertise in project management, the AuthentiCare solution for Electronic Visit Verification (EVV), quality assurance, independent verification and validation, development, and training services to government health and human services agencies. In the past 20 years, he has managed teams of IT professionals in the areas of analysis, design and development of new technology solutions, project management and oversight, cost-benefit analysis, and system design and performed Independent Verification & Validation. Mr. Sullivan has experience with multi-year projects of varying size and complexity with the largest valued at $440 million. The larger, more complex projects included working with multiple vendors to achieve successful project outcomes.

Key – Quality Manager: Cayle Cox

Mr. Cox is an experienced Information Technology and Product Management professional with over 10 years of system implementation, quality management, project management, relationship management, people management, operations management (including escalation/incident management), and client service experience. He holds both an MBA and a bachelor's degree. For 10 years, Mr. Cox was in the First Data Global Command Center, where he supported every production system deployed in the United States, Canada, and Mexico. He also managed Security and Fraud products, where he focused on fraud case management products that processed over 70 million cases annually. Since October 2019, Mr. Cox has been dedicated to the support of AuthentiCare projects in a quality management capacity.

Executive Oversight: King Farias

As a value-added resource to support the West Virginia EVV project, FDGS is proposing an Executive Oversight role to provide project coordination and allow for a single point of contact for the Department when executive escalation is required. FDGS proposes King Farias in an Executive Oversight capacity. As the National Director of our AuthentiCare delivery organization, Mr. Farias provides executive management, strategic vision, and a clear escalation path for the full team. He brings more than 10 years of technical and project management experience on all phases of the Software Development Life Cycle (SDLC) and excels at building relationships, as well as status reporting to executive leadership, customers, and staff. He specializes in implementations and cyber security and holds multiple certifications including: PMP, CISSP (Certified Information System Security Professional), Scrum Master, and Scrum Product Owner, as well as multiple cloud certifications.

Mr. Farias will work closely between the AuthentiCare team, DHHR, and the technical resources within FDGS that support the application and provide operational support. This combined team provides solid expertise in the AuthentiCare solution, its development and implementation, and the client services needed to support West Virginia EVV.

3.2.1 Resumes

We have provided brief resumes for key personnel on the following pages. The resumes clearly detail each key team member's role and their specific expertise in EVV and the AuthentiCare solution. For our proposed key staff, we have completed RFP Table 24 with three references to successfully demonstrate their experience and capabilities meeting the requirements of this RFP. Our proposed team brings experience on multiple statewide implementations similar in size and scope to this RFP and the West Virginia EVV project. The key personnel identified in this proposal will be ready to start on Day One.

FDGS includes resumes for the following key personnel:

- **Account Manager**: Asad Salahuddin
- **Project Manager**: David Sullivan
- **Quality Manager:** Cayle Cox

In addition to the required resumes of our key personnel, we are also including the resume of Mr. King Farias, Executive Oversight. While not part of the key personnel, FDGS noted the importance of this role to maintain oversight of the West Virginia EVV project.

King Farias, Executive Oversight



Program Expertise

- Cloud Strategy
- Business Intelligence/Analytics

Specializations

- Cyber Security
- Implementation

Education and Memberships

- St. Edwards University (2007)

Certifications and Licenses

- CISSP (2017)
- PMP (2017)
- AWS Certified Cloud Practitioner (2017)
- AWS Certified Solutions Architect (2017)
- AWS Certified Developer (2017)
- Scrum Master (2017)
- Scrum Product Owner (2017)

Professional Summary

Mr. Farias is a results-driven Senior Technology and Security Professional with expertise in design, development, and delivery of critical IT security operations across large financial institutions and corporations. He has an aptitude for eliciting complex requirements and translating organizational objectives into highly resilient, scalable IT and security solutions. Mr. Farias is regarded as a thought leader with a strong record of successfully engaging strategic partners to align goals, define vision, and engineer solutions to protect the integrity of critical information systems. He is adept at leveraging sound business and technical acumen to build and lead high-performance teams that execute on global business strategies. Mr. Farias holds multiple certifications including: PMP, CISSP, Scrum Master and Product Owner, and several AWS certifications.

Experience

First Data

AuthentiCare Implementation Projects: National Director, 06/10/2019 – Present

Mr. Farias is responsible for National AuthentiCare Delivery solutions to state and federal clients.

- Leads systems integration team comprised of client relationship managers, business analysts, project managers, trainers, industry subject matter experts, and quality assurance analysts.
- Partners with First Data product teams to ensure successful delivery of client solutions.

Trusted Forge

Texas Bulk Electric Grid System: Chief Solutions Architect, 04/2018 – 05/2019

Mr. Farias managed FTE and contract resources for critical infrastructure projects for the Texas Bulk Electric Grid System, ERCOT. He was responsible for delivering solution compliance within NERC Critical Infrastructure Protection standards.

- Provided Cybersecurity and Enterprise Architecture cloud-based solutions based on TOGAF, SABSA, ITIL and COBIT frameworks, in compliance with related ISO standards.
- Directly led and managed five major implementation programs based on Enterprise Joint Security Operations, Human Capital Investment, Cloud Strategy, Business Intelligence & Analytics, ITIL Service Management, and Enterprise Automation.

First Data

Global Service Assurance: Director, Client Services & Support, 04/2015 – 04/2018

Mr. Farias managed a team of 12 direct reports and over 40 indirect reports globally. He led all aspects of the Global Service Assurance program and defined the information assurance framework for technology strategies in alignment with business and stakeholder objectives.

- Served as Production Assurance Director for Global Financial Services (GFS) and Electronic Security Solutions (ESS) LOBs.
- Led program to globalize the Client Services and Support organization by creating a follow-the-sun model for IT security and Infrastructure operations across the US, Europe, and Asia Pacific
- Directed the design and implementation of the Global Client Services & Support Service Management Infrastructure and Operations departments, worked closely with senior executive leadership to ensure fulfillment of critical objectives and project milestones

J.P. Morgan Chase & Co.

Vice President, Infrastructure Support Services, 04/2012 – 04/2015

Mr. Farias managed a team of 5 direct reports and over 60 employees and contractors delivering global infrastructure services for millions of JPMC customers.

- Set up the critical infrastructure program and deployed global technology enhancements which improved performance of critical applications across Europe and Asia Pacific and delivered 40 percent cost reduction with 25 percent reduction in headcount.

Table 23: Resumes for Proposed Key Staff

Table 3.3 summarizes the qualifications of our proposed key staff for West Virginia's EVV project based on the scope of work detailed in this RFP. The two-page resumes for each role follow with additional work experience – offering DHHR a leadership team with proven success delivering projects of similar size and scope specific to electronic visit verification solutions.

Table 3.3 – Proposed Key Staff Meet or Exceed all Required Qualifications

Name	Proposed Role	Experience in Proposed Role
Asad Salahuddin	**Account Manager**	Mr. Salahuddin meets or exceeds all qualifications required from RFP Table 8: Staff Qualifications, Experience, and Responsibilities including: • More than 15 years of experience and management of state Medicaid, health services, and EVV projects in the Home and Community Based Services (HCBS) programs • Master of Business Administration (MBA) from The American University • Knowledge and application of the Medicaid program business rules and procedures • Experience of EVV and similar programs statewide programs including WIC, EBT, and ECC • Five years of experience specific to EVV systems including fee-for-service (FFS) and claims processing in Nevada, New Mexico, and Oklahoma, which required complete understanding of the policies and administrative rules for each.
David Sullivan	**Project Manager**	Mr. Sullivan meets or exceeds all qualifications required from RFP Table 8: Staff Qualifications, Experience, and Responsibilities including: • Is a Project Management Professional (PMP®) through the Project Management Institute (PMI) • Project Manager on multiple EVV projects for FDGS • Thirteen years of project management experience of IT projects with an additional six years in lead and senior project positions • Over 19 years of health and human services related experience • Proven ability to manage both people and process successfully in a wide range of project types and sizes
Cayle Cox	**Quality Manager**	Mr. Cox meets or exceeds all qualifications required from RFP Table 8: Staff Qualifications, Experience, and Responsibilities including: • Bachelor of Arts from the University of Nebraska and MBA from Bellevue University • More than 10 years of experience in quality assurance and security assurance for multiple projects and products • Eight years as Command Center Manager (comparable to Quality Manager role and responsibilities from RFP Table 8) responsible for and providing oversight of all aspects of claims and data management as implemented and delivered by more than 20 direct reports

Asad Salahuddin, Account Manager



Program Expertise

- Medicaid
- Electronic Visit Verification
- Managed Care Organizations
- Electronic Benefits Transfer
- Electronic Child Care

Specializations

- Account Management
- Team Leadership
- Training/Onboarding
- Software DDI
  - ✓ AuthentiCare
- SLA Electronic Claims and Payments
- Annual Transaction Revenue
- Product Technical Enhancements and Updates

Education and Memberships

- M.B.A., Marketing
  The American University
- B.A., Economics
  The College of Wooster

Certifications and Licenses

- PMP Certification, 2009
- ITIL Certification, 2010

Professional Summary

Mr. Salahuddin has over 15 years of experience leading successful state agency initiatives in account management and client relationship capacity and extensive Electronic Visit Verification (EVV) Subject Matter Expertise. He has provided account management for FDGS's New Mexico EVV project with four of the largest Managed Care Organizations (MCO) in the country, and in Nevada and Oklahoma as well. As an Account Manager with FDGS, Mr. Salahuddin has led the development, documentation, design, testing, and implementation of the AuthentiCare/EVV project in New Mexico. He has provided onboarding and onsite training with state officials and advocacy groups, product enhancements, and managed EVV revenue inflow of $1.5M annually. In addition to knowledge and application of the Medicaid program business rules and procedures, Mr. Salahuddin has experience in client management, electronic application designs and enhancements, and provider training.

Qualifications for This Role

- Master of Business Administration (MBA) degree and PMP certification
- Over 15 years of Contract Manager experience serving multiple state agencies in Human Services departments
- Five years of EVV experience
- Five years of Medicaid/Healthcare experience including knowledge of Medicare EVV claims processing
- Knowledge of HCBS delivery including EVV, WIC, EBT, and ECC

Experience

First Data Government Solutions, LP

Nevada Electronic Visit Verification Project: Account Manager, 04/2019 – Present

New Mexico (NMCC) Electronic Visit Verification Project: Account Manager, 08/2014 – Present

Oklahoma Electronic Visit Verification Project: Active Project Engagement

Mr. Salahuddin provides account management oversight, monitors project progress, and coordinates the team's client needs and resource allocations for the states of Nevada, Oklahoma and New Mexico. He provides account management throughout the life of each contract. He monitors client, customer, and provider satisfaction; reduces administrative barriers for the provider; and improves the ease of use and access. His responsibilities involve providing primary client support for the application. Mr. Salahuddin plays a central role in the oversight of the development, documentation, design, and testing of the AuthentiCare application. He coordinates and participates in weekly and monthly status calls with the State and providers and supports client relationships. He provides application support and works with the State on the implementation of any future enhancements to the AuthentiCare product. Mr. Salahuddin brings extensive knowledge of the Medicaid program business rules and procedures.

Capgemini USA

North America Infrastructure Services: Program Manager, 05/2013 – 08/2014

Mr. Salahuddin managed multiple Texas state agencies and their infrastructure implementation projects in the Texas DIR Data Center Services contract. Responsibilities included: portfolio management ($30M revenue); change and risk management; relationship management; and process improvement including solution, cost, and new acquisitions.

Affiliated Computer Services INC. (ACS, A Xerox Company)

National Retail Operations: Service Delivery Manager/Director, 03/2010 – 02/2013

Mr. Salahuddin managed the national retail operations for EBT, WIC, and Electronic Child Care (ECC) including EBT vendor contract processing operations, EBT and ECC vendor help desk operations, and the Point of Sale (POS) National Depot facility. He managed a team of 30 direct reports and was responsible for all P&L and cost optimization in EBT vendor contract processing, POS procurement, inventory tracking and recovery/recycling measures. He managed business relationships and provided support and problem resolution for EBT and ECC programs in Michigan, Louisiana, Texas, Ohio, North Carolina, and Virginia.

Texas Department of State Health Services (DSHS)

WIC EBT implementation: Project Manager/Consultant, 05/2005 – 09/2009

Mr. Salahuddin managed the statewide offline WIC EBT implementation at 2,200 WIC retailers using POS terminal and smart card technology. Responsibilities included: Relationship Manager to WIC transaction processors for DSHS, POS installation status reports to stakeholders, matrix management of state employees during statewide project implementation, and monitored compliance to DSHS standards for all POS processes and managed stakeholder relationships.

David Sullivan, Project Manager



Specializations

- Project Management
- Quality Assurance
- Design, Development, & Implementation
- Cost Benefit Analysis
- System Design
- Independent Verification & Validation

Certifications and Licenses

- PMP
- CSM

Methodologies

- Agile
- Waterfall
- PMBOK

Professional Summary

Mr. Sullivan is a Certified Project Management Professional and Certified Scrum Master with expertise in project management, quality assurance, independent verification and validation, development, and training services to government health and human services agencies. In the past 20 years, he has managed teams of IT professionals in the areas of analysis, design and development of new technology solutions, project management and oversight, cost-benefit analysis, and system design and performed Independent Verification & Validation. Mr. Sullivan has experience with multi-year projects of varying size and complexity with the largest valued at $440 million. The larger, more complex projects included working with multiple vendors to achieve successful project outcomes.

Qualifications for This Role

- Project Management Professional Certification (PMP)
- Thirteen years' project management experience with an additional six years in lead and senior project positions
- Over 19 years of health and human services related experience
- Proven ability to manage both people and process successfully in a wide range of project types and sizes

Experience

First Data Government Solutions, LP

AuthentiCare Palco Jurisdiction Portfolio Project Manager, 06/2019 – Present

The AuthentiCare solution for Electronic Visit Verification (EVV) tracks in-home visits made by employees or contractors to provide services. Benefits with statewide EVV implementations helps human services agencies ensure customers receive their services.

FDGS was asked to implement and manage an Electronic Visit Verification (EVV) Solution for the State of Pennsylvania, for the State of Colorado, and for the State of Kansas on Palco's behalf. AuthentiCare is a hosted product where the Provider, Customer and Client staff will access and use FDGS' Software-as-a-Service (SaaS) solution.

AuthentiCare New Mexico Early Prevention Screening Diagnostic and Treatment (EPSDT) Project Manager, 06/2019 – Present

Health Care Service Corporation requested that FDGS implement the Early Prevention Screening Diagnostic and Treatment (EPSDT) services in FDGS' AuthentiCare platform in compliance with the 21st Century Cures Act. This would include adding and configuring children's personal service to the existing AuthentiCare platform.

Additional Experience

- FDGS: Nebraska Department of Health & Human Services Eligibility & Enrollment Solution Independent Verification & Validation Project, Senior IV&V Analyst, 04/2015 – Present
- FDGS: Hawaii Tax System Modernization, Senior IV&V Analyst, 09/2018 – 06/2019
- FDGS: Louisiana Department of Children and Family Services Transformation Project
- PMO UAT Lead, 07/2012 – 04/2013
- Catholic Health Initiatives, EPMO: Physician and Clinical Services Various Projects, Senior Project/Program Manager, 04/2013 – 04/2015
- Software Engineering Services (SES)
- Senior Project Manager/Project Consultant, 12/2005 – 07/2012
- Veterans Administration Central Iowa Healthcare System (VA CICHS)
- Florida Department of Revenue Independent Verification & Validation Software Engineering Services 12/2008 – 03/2012
- Douglas Omaha Technology Commission (DOT.Comm) SES Corporate PMO
- Mutual of Omaha Various Projects Lead Analyst/Project Manager, 05/2000 – 12/2005

Cayle Cox, Quality Manager



Specializations

- Project Management
- Product Management
- Quality Management
- Relationship Management
- Case/Claim Processing
- Data Management

Education and Memberships

- B.A., Telecommunications Management, University of Nebraska
- M.B.A., Bellevue University

Professional Summary

Mr. Cox is an experienced Information Technology and Product Management professional with over 10 years of system implementation, quality management, project management, relationship management, people management, operations management (including escalation/incident management) and client service experience. He holds both an MBA and a bachelor's degree. For 10 years, Mr. Cox was in the First Data Global Command Center, where he supported every production system deployed in the United States, Canada, and Mexico. He also managed Security and Fraud products, where he focused on fraud case management products that processed over 70 million cases annually. Mr. Cox is now dedicated to the support of AuthentiCare projects in a quality management capacity.

Qualifications for This Role

- Master of Business Administration, a bachelor's degree in telecommunications, and 12 years of experience in a healthcare-related industry.
- Twelve years providing quality management on large-scale, complex projects as large as or larger than West Virginia's. Includes responsibility for the management of day-to-day operations, testing, and participation in relevant meetings.
- Eight years as First Data Command Center Manager responsible for and providing oversight of all aspects of claims and data management as implemented and delivered by more than 20 direct reports in support of every production system deployed in the United States, Mexico, and Canada.

Experience

First Data Government Solutions, LP

Director, Quality Management, AuthentiCare, 10/2019 – Present

Mr. Cox executes continual improvement methodologies throughout the AuthentiCare delivery lifecycle with special focus on IT development processes, application testing, training, and Help Desk support involving issue management and resolution. He is responsible for functional tests on all UAT deployments prior to client engagement and serves as a project manager and business analyst for various AuthentiCare projects. This experience includes firsthand experience in all deployment phases.

Product Manager: Security and Fraud, 05/2018 – 10/2019

Mr. Cox has been the product owner for case management tools that process over 70 million cases per year. Systems included the Fraud Detection Work Center, the Predictive Dialer, and the Lost/Stolen GUI. He was the fraud call processing service owner and responsible for quality management, including principal case/claim management point of contact for client escalation, RFPs, and system outages. Mr. Cox was also the P&L owner for fraud call processing services and fraud case management products.

Service Assurance Analyst, 01/2016 – 05/2018

Mr. Cox was the Globalization Lead for the Command Center's Globalization project. This project implemented a two-site, follow-the-sun model that saved millions in operating expenses while guaranteeing consistent tools and processes throughout the globe. Mr. Cox executed quality management methods to provide leadership, training, and mentoring on migration strategies. He facilitated and managed the engagement of internal and external stakeholders and monitored tasks and project assignments while ensuring project deliverables were met and that schedule changes were addressed and communicated. He also managed projects that addressed all components of the ITIL model while ensuring compliance with data privacy laws between countries and analyzed feedback on project effectiveness and assist with providing solutions to ensure stakeholder success.

Command Center Manager, 04/2008 – 01/2016

Responsible for both project and relationship management, Mr. Cox served as the department lead for the Denver Command Center closure project. This multi-year project reduced head counts by 40 percent and saved millions in operating expenses without reducing service quality. Quality Management was involved in every aspect of Command Center management, which included Incident Management, Merchant Services, Financial Services, and Batch processing. Mr. Cox hired and trained 50 new operators and oversaw the migration of tools to the new site while averaging 20 direct reports. He finished each project phase on time and under budget and maintained current knowledge of the organization, technology, and business objectives. Mr. Cox was the primary point of contact for technical escalations for both internal and external clients. He served as client advocate during system outages, contributing as the liaison between the organization and impacted clients. As relationship manager he received multiple internal awards for outstanding client support. He monitored online and batch functions on multiple midrange and distributed platforms while communicating potential and actual impacts to clients.

3.2.2 References

Table 3.4 – Key Personnel References for Proposed Account Manager (RFP Table 24)

Key Personnel Reference Form							
Key Personnel Name:	Asad Salahuddin	Proposed Role:	Account Manager				
Reference 1							
Client Name:	Presbyterian HealthCare	Client Address:	9521 San Mateo Drive, Albuquerque, NM 87113				
Contact Name:	Brittney Maldonado	Contact Title:	Long Term Care Director				
Contact Phone:	505-923-5765	Contact E-mail:	bmaldonad2@phs.org				
Project Name:	New Mexico EVV		Start Date:	MM/YYYY 04/2014	End Date:	MM/YYYY Present	
Project Description: Implementation and Operations phase of the NM EVV project for Presbyterian Health Services (PHS), one of the largest MCOs in New Mexico. New Mexico is an MCO model for EVV and FDGS is the sole EVV provider for the state.							
Project Role and Responsibilities: Served as the Implementation Manager and the Account Manager for PHS for the NM EVV project. This is still an active EVV account for FDGS and I manage this account presently.							
Reference 2							
Client Name:	OptumCare	Client Address:	2716 N. Tenaya Way, Las Vegas, NV 89128				
Contact Name:	Curt Schatz	Contact Title:	Vice President, IT Operations and Strategic Initiatives				
Contact Phone:	505-280-5528	Contact E-mail:	curt.schatz@optum.com				
Project Name:	New Mexico EVV		Start Date:	MM/YYYY 04/2014	End Date:	MM/YYYY Present	
Project Description: Implementation and Operations phase of the NM EVV project for United Health Care (UHC) of New Mexico. New Mexico is an MCO model for EVV and FDGS is the sole EVV provider in the state.							
Project Role and Responsibilities: I served as the Implementation Manager and the Account Manager UHC for the NM EVV project. NM is still an active EVV account for FDGS and I manage this account presently.							
Reference 3							
Client Name:	BlueCross and Blue Shield New Mexico	Client Address:	5701 Balloon Fiesta Parkway NE Albuquerque, NM 87113				
Contact Name:	Quinn Glenzinski	Contact Title:	Senior Director of Provider Network				
Contact Phone:	505-816-4181	Contact E-mail:	quinn_glenzinski@bcbsnm.com				
Project Name:	New Mexico EVV		Start Date:	MM/YYYY 04/2014	End Date:	MM/YYYY Present	
Project Description: Implementation and Operations phase of the NM EVV project for BlueCross BlueShield (BCBS) New Mexico. New Mexico is an MCO model for EVV and FDGS is the sole EVV provider in the state.							
Project Role and Responsibilities: Served as the Implementation Manager and the Account Manager for BCBS for the NM EVV project. NM is still an active EVV account for FDGS.							

Table 3.5 - Key Personnel Reference Form for Project Manager (RFP Table 24)

Key Personnel Reference Form						
Key Personnel Name:	David Sullivan	Proposed Role:	Project Manager			
Reference 1						
Client Name:	Mutual of Omaha	Client Address:	Mutual of Omaha Plaza Omaha NE 68175			
Contact Name:	David Kern	Contact Title:	Manager of Project Managers			
Contact Phone:	402-980-5298	Contact E-mail:	Kernat2104@cox.net			
Project Name:	Multiple Projects		Start Date:	MM/YYYY 05/2000	End Date:	MM/YYYY 01/2006
Project Description: Multiple Projects spanning implementing new processes through developing and implementing a new proposal and insurance rating solution, which earned national recognition for the best use of technology in the insurance industry						
Project Role and Responsibilities: Overall project manager						
Reference 2						
Client Name:	State of Nebraska	Client Address:	Golds Building Lincoln NE			
Contact Name:	Ed Petrick	Contact Title:	Project Manager			
Contact Phone:	402-968-4461	Contact E-mail:	Ed.Petrick@cox.net			
Project Name:	NE ESS NTRAC		Start Date:	MM/YYYY 04/2015	End Date:	MM/YYYY 08/2018
Project Description: NE DHHS contracted to have a Medicaid enrollment and eligibility solution developed and implemented by a third-party System Integrator.						
Project Role and Responsibilities: Senior IV&V analyst working with NE DHHS and the System Integrator to review project artifacts to ensure contractual and CMS compliance -- verifying the correct thing was done and done to correct way						
Reference 3						
Client Name:	Iowa Department of Veterans Affairs	Client Address:	3600 30t St, Des Moines, IA 50310			
Contact Name:	David West	Contact Title:	Senior Business Analyst			
Contact Phone:	402-298-5624	Contact E-mail:	DWest870@gmail.com			
Project Name:	Enterprise Reporting Solution		Start Date:	MM/YYYY 03/2010	End Date:	MM/YYYY 04/2011
Project Description: Create a reporting solution to capture and analyze defined key performance indicators						
Project Role and Responsibilities: Overall project manager including managing staffing budget and performance						

Table 3.6 - Key Personnel Reference Form for Quality Manager (RFP Table 24)

Key Personnel Reference Form						
Key Personnel Name:	Cayle Cox	Proposed Role:	Quality Manager			
Reference 1						
Client Name:	Citibank	Client Address:	6460 Las Colinas Blvd Irving, TX 75039			
Contact Name:	Ramakumar Chalasani	Contact Title:	Program Manager			
Contact Phone:	469 220 8948	Contact E-mail:	ramakumar.chalasani@citi.com			
Project Name:	PR18016584 - Modify Existing Web Services		Start Date:	MM/YYYY 08/2018	End Date:	MM/YYYY 05/2019
Project Description: In August 2018, CITI requested a direct connection to First Data's Fraud Suspect Queue. CITI wanted access to this DB2 table so they could use its data to send fraud notification via an external notification engine. I had to reject CITI's initial request because it would have put other clients at risk, exposed proprietary information, and weakened our product offering. Instead of walking away from this request, I told CITI that I would use their business case to create a new service. I worked with internal development teams to design a technical solution capable of sending transactions to our clients within three seconds of authorization. I also consulted our capacity team to ensure our system was capable of sending over 50,000 transactions per month, obtained approval from our legal team, and established a pricing structure. Finally, I met with various members at CITI to explain the strategy and I was ultimately able to obtain their approval. In the end, my solution protected all clients from unnecessary exposure and outages and solved CITI's business objective.						
Project Role and Responsibilities: Product Manager						
Reference 2						
Client Name:	CO-OP Financial Services	Client Address:	9692 Haven Avenue Rancho Cucamonga, CA 91730			
Contact Name:	Chris Dean	Contact Title:	VP, Fraud Solutions			
Contact Phone:	(310) 691-9643	Contact E-mail:	Chris.Dean@coop.org			
Project Name:	CO-OP Fraud SMS Notification Enhancement request		Start Date:	MM/YYYY 02/2019	End Date:	MM/YYYY 05/2019
Project Description: This project was similar to the CITI project listed above. CO-OP asked First Data to create a business offering that would enable an external notification engine to send fraud notifications to clients within seconds of a transaction being declined. CO-OP also wanted to load transactions automatically into their IVR and load their Business Intelligence database. I proposed a similar approach to what I developed for CITI and CO-OP accepted my proposal. The unique aspect of this project is that CO-OP had already been working with our internal group in charge of external notifications for over a year and they were not getting the results they needed. Rather than pushing CO-OP down a path that was clearly not meeting their needs I proposed a solution that gave them more control and faster response times. CO-OP accepted my proposal and began actively pursuing this solution.						
Project Role and Responsibilities: Product Manager						
Reference 3						
Client Name:	Home Credit	Client Address:	6240 Sprint Pkwy, Overland Park, KS 66211			
Contact Name:	Stacey Wishowsky	Contact Title:	Director of Fraud Operations			
Contact Phone:	302-229-7162	Contact E-mail:	Stacey.wishowsky@experian.com			
Project Name:	Bridge processing call processing for Home Credit		Start Date:	MM/YYYY 12/2017	End Date:	MM/YYYY 01/2019
Project Description: Before I joined the Fraud Product Team Home Credit was setup on a failed offering called "bridge processing." The idea behind this solution was that call center agents would review transactions prior to client contact and if contact was necessary then an automated dialer would contact the client. The problem was this						

solution did not work correctly because the dialer was unable to close "bridge" cases. When the "bridge processing" project was implemented, Home Credit clients received hundreds of unwanted automated calls. This failed process strained our relationship with Home Credit and it cost FDGS thousands of dollars in SLA penalties. When I joined the Fraud team approximately five months after this project was implemented our relationship was still strained. I spent a significant amount of time improving agent performance and addressing all of Home Credit's concerns with FDGS' quality. Over the course of a few months, I was able to rebuild this relationship and in January 2019 Home Credit's was moved back to standard billing rates.
Project Role and Responsibilities: Product Manager

4.0 Attachment 5: Initial Work Plan

RFP Section 5.4.2.10 (Table 11) & Attachment 5, pp. 74, 115
1.1 The Vendor should provide an Initial Work Plan.
1.2 At a minimum, the Vendor's proposed Initial Work Plan should include the following:
1.2.1 Detailed tasks and timelines, outlining the major project phases planned by the Vendor. These should include, at a minimum, the timeline and tasks associated with full deployment of functionality, including:
1.2.1.1 Responsibilities
1.2.1.2 Timelines and Durations
1.2.1.3 Milestone Dates
1.2.1.4 Deliverable Dates
1.2.1.5 Vendor personnel hours by deliverables for each project phase
1.2.1.6 Department of Health and Human Resources (DHHR) personnel hours by phase deliverable
1.2 1.7 All critical dependencies for the project's milestones and deliverables
1.2.2 Work Breakdown Structure (WBS) organized by project phase and task group defined in Section 4.6: Project Task Groups and Deliverables of this request for proposal (RFP)
1.2.3 Project Schedule for all project deliverables and milestones
1.2.4 Identification of resources assigned the responsibility for each deliverable within the WBS to the level at which control will be exercised
1.2.5 Identification of deliverables that require a more prompt DHHR acceptance than described in the RFP, including the proposed acceptance period for the deliverable
1.3 The Initial Work Plan should be provided as an attachment to the Vendor's Technical Proposal and tabbed as such in the submission.

FDGS recommends a phased implementation, with Phase 1 achieving 21st Century Cures Act compliance by January 1, 2021, and establishing the basis for CMS certification.

Attachment 7: Business Specifications Approach asks that if the Vendor is proposing a phased implementation, the Vendor should indicate how that approach may or may not affect functionality. Addendum 6 of this RFP, Q133, indicates that DHHR will consider vendors who propose a phased implementation approach.

FDGS maintains EVV and CMS program and policy experts. Our subject matter experts have examined the RFP to develop our solution and assess the requirements included in this RFP. With an aggressive implementation period of only six months, FDGS has determined that a focused approach to Go Live is necessary. Our approach focuses on the necessary requirements, features, and functions of the AuthentiCare EVV implementation to:

1. Verify and validate all EVV capabilities are included to fully comply with the 21st Century Cures Act
2. Include all requirements and capabilities needed to certify West Virginia's EVV solution CMS according to their Outcomes Based Certification guidelines and processes

With this focused approach to the initial implementation period, FDGS will work with the Department to validate all requirements necessary for Go Live, iteratively complete the design and configuration specific to West Virginia's program policy, and deploy a fully functional EVV solution.

Upon award, FDGS will lay out an initial plan for proposed future releases to include the additional features and functions necessary to support the remaining requirements noted as "Will Meet" in Appendix 1 – Detailed Specifications.

To detail this approach, FDGS has included its Initial Work Plan in Proposal Section 4.1. In addition to the Initial Work Plan, FDGS has included an abridged Project Management Plan

(PMP) in Proposal Section 4.2. The updated PMP will include the sub-plans of the PMP that are required for deliverables D002 through D013. The abridged PMP and initial work plan complement each other to form our overall approach to the EVV project. The FDGS team will expand, review, and submit both plans and the PMP sub-plans to the Department for formal approval following the Project Kickoff Meeting (D001). We will execute all Deployment Task activities and services in accordance with the approved contract and Project Management Plan (PMP).

FDGS will provide project management of tasks and deliverables for the EVV project, including the day-to-day management and administrative support of staff and activities. Using FDGS' experience from 11 statewide EVV implementations, we will assist DHHR with identifying roles and activities necessary for the Department to successfully implement and operate the EVV solution. FDGS will assist DHHR in coordinating assignments for State staff working on the EVV project. Throughout the EVV project, the FDGS Project Manager will employ project management techniques to confirm that the PMP is developed, executed, monitored, reported on, and maintained to achieve project success.

At the beginning of this EVV project, the abridged project schedule included in this response will be expanded by FDGS and submitted for review and approval by Department sponsors and stakeholders. FDGS understands that the project work plan is subject to input and final approval by DHHR. See Figure 4.1 to see how the Project Work Plan reflects an AuthentiCare implementation that consists of six phases: Initiation, Planning, Configuration, Deployment, Operations, and Closing.

The AuthentiCare EVV Implementation Methodology aligns to the Project Task Groups, the Payment Milestones, and the deliverables included in each milestone defined within the RFP. This introduction describes the major activities that occur in each phase of the project. Our EVV work plan includes the major phases, milestones, tasks, and timelines mutually agreed following Project Kickoff Meetings.

As the project details are finalized, FDGS will map the appropriate deliverables to our standard AuthentiCare system and project deliverables so that all required deliverables are accounted for in the expanded project work plan.

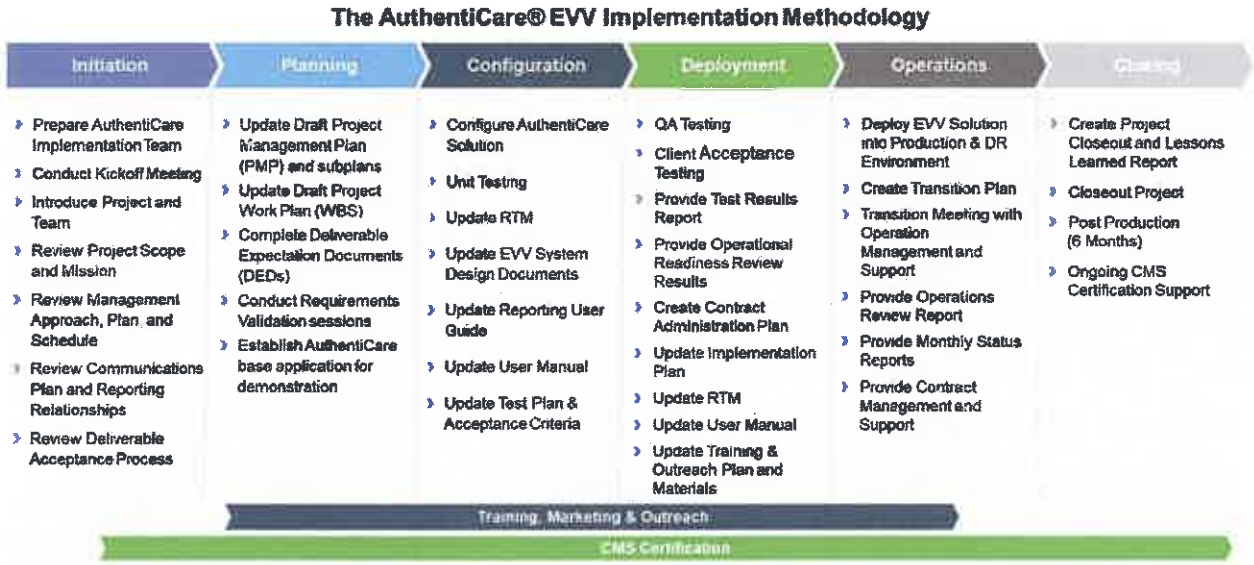


Figure 4.1 – EVV Implementation Approach and Activities by Phase

Initiation Phase

Initiation

After contract execution, the FDGS team will conduct the onsite client kickoff meeting. The project initiation phase kicks off project/iterations and involves defining the project objectives, scope, schedule, purpose, and deliverables to be produced. In this phase all stakeholders and the FDGS Team are identified and roles/responsibilities are assigned. The project initiation phase is a key phase to confirm alignment with Department goals and objectives and overall project success.

Planning Phase

Planning

The FDGS Team confirms that the project's strategic goals are met by verifying that project management disciplines are planned and performed according to best practices and defined in the Project Management Plan (PMP). The FDGS Team will facilitate a joint review of RFP requirements with DHHR and designated business and policy stakeholders, resulting in an approved baseline EVV Solution Requirements Traceability Matrix (RTM). During the joint review of the requirements, FDGS will demo the EVV solution to show how it satisfies the requirements, identify configurable features and functions, and identify any customizations required in the EVV solution.

In the planning phase, using the RTM, AuthentiCare Design Sessions are held with the stakeholders and key members of the FDGS team including the delivery team to clarify, prioritize, and detail the components of the baseline System Integration Plan (SIP) and business rules of the DHHR AuthentiCare solution. The purpose of the sessions is to finalize the implementation plan and to define system configuration items. At the end of the sessions, there will be a set of project deliverables including a project management plan, project schedule, test plan, deployment approach, and training approach, to clearly define project scope and establish a clear understanding of roles and responsibilities by stakeholders and the FDGS Team. The deliverables will be provided to DHHR for review and approval.

This EVV configuration and detailed system design documentation is comprised of:

- System Integration Plan (SIP)
- Appendix B (Imports/Exports)
- Appendix C (IVR Script)
- Appendix D (Language Packet)
- Appendix S (Web Services), if necessary

The SIP and AuthentiCare Detailed System Documentation must be approved by DHHR prior to the initiation of the Configuration and Development phase.

Configuration and Development Phase



In the Configuration Phase, specific system configuration items are identified and documented in the AuthentiCare detailed system design documents, implemented by our technical team, and unit tested to verify that they meet DHHR's needs and expectations.

This configuration implementation, along with the unit, QA, and User Acceptance Testing, is done in coordinated cycles as an iterative approach to allow flexibility, alignment, and clarity between FDGS and DHHR as the project progresses instead of traditional development cycles where all functionality is delivered at once. This iterative approach improves the final delivered product as well as the customer experience.

Deployment Phase



Deployment consists of promoting the configured system through:

- Quality Assurance Test environment for FDGS Quality Assurance Testing
- Client Acceptance Test environment for User Acceptance Testing

The Deployment Phase involves activities related to preparing the system for production processing in a live state. System readiness activities are performed in advance of the production launch date, including the import of production data, final production system validation and formal system acceptance. The FDGS Team is dedicated to providing the necessary support for a smooth and successful launch.

Training will be provided for DHHR staff, providers, and other users beginning in the Deployment Phase according to the agreed-upon Training and Outreach Plan, which is expected to continue past go-live.

Deployment phase results in a request for DHHR to sign off that the application is ready for FDGS to migrate the overall solution into production. With this confirmation and formal approval from the Department (and CMS), FDGS' governance processes are initiated to confirm and verify that all pre-implementation checklist items are planned and completed before the Go/No-Go decision point.

For each of the critical tasks and activities planned for implementation, cutover, and post-production readiness, FDGS uses its proven checklists to verify and validate all technical and organizational resources are ready to use the new EVV.

Operations Phase



Once acceptance is received from DHHR, we initiate production readiness tasks that involve implementing the system and importing data into the production environment. FDGS' recommended approach is to conduct a soft go-live where providers can validate client, provider, and worker demographic data, as well as authorizations.

At this stage, the newly configured AuthentiCare solution for DHHR is ready for full production cutover. The FDGS Team verifies that DHHR, stakeholders, your provider community, and other users have the necessary support for a smooth and successful launch of the solution.

During the agreed cutover period, the FDGS implementation team will transition the project oversight of the WV EVV system to our Account Manager and Operations Manager for the day-to-day operation of the system. We also engage the FDGS Global Service Delivery team for ongoing customer service support. Members of the support team are introduced and trained during the implementation phase to ramp up operational support. New team members will attend meetings and on-site events when needed to continue to gain knowledge and start developing relationship for continued support and maintenance.

During the first 30 days of a production rollout, the FDGS Delivery Team will stay engaged remotely to maintain close contact with the stakeholders and the provider community. Any issues or program adjustments that surface during this transition will be discussed in detail with the stakeholders prior to implementing any production changes. The project will be officially transitioned to the Client Services team.

Implementation Closeout Phase

A post-implementation review is performed to verify all requirements have been met and results from the Lessons Learned session are formally documented. Upon successful transition to the Maintenance and Operations Phase, the Project Manager will begin the closeout activities of the implementation project and receive final acceptance from DHHR.

Overall EVV Approach

The FDGS approach to EVV services projects and high-level Gantt chart, shown in Figure 4.4, incorporates a proven project timeline and schedule to meet the projected Go-Live target of January 1, 2021. This proposed timeline provides a repeatable, high-level approach that we tailor to your requirements and adjust based on the final, agreed-upon contract dates and review periods between DHHR and FDGS. DHHR personnel and stakeholders will be identified and participation from DHHR staff is crucial when working under a compressed timeline as required by the State.

Our AuthentiCare EVV solution offers the ability to quickly and efficiently move through the design, configuration, and testing phases based on functional areas of providers, members, workers, authorizations, visits, claims, and reporting with unit, functional, system integration, interface, regression and user acceptance testing at each milestone. This will support the aggressive timeline requested and allow for enhancements to begin shortly after the initial implementation proposed for January 1, 2021.

Testing scenarios are developed internally for our Testing Center of Excellence (TCoE) pool of resources and those test scenarios will be shared with DHHR. If necessary, additional test

scenarios will be provided by DHHR to include specific examples of real-life situations are executed during the test cycles. End-to-end testing will be completed by both DHHR and FDGS before the final demonstration.

FDGS assigns a dedicated Project Manager for each AuthentiCare implementation. The Project Manager is the primary contact for DHHR and is available throughout the project to answer questions from all stakeholders, monitor and communicate project progress, coordinate the team's needs, maintain the schedule, identify risks and issues, and manage resource allocation. We also assign an Account Manager to support the resolution of project and operational issues. The Project Manager transitions overall responsibility to the Account Manager during the Closeout phase of our implementation plan and transition to Maintenance and Operations (M&O). Since the Account Manager has been a part of the project since the start of the initiation phase, there is continuity of communications and relationship to verify that post-implementation activities are executed without delay, interruption, or impediments. This approach has been tested and proven effective in past statewide and MCO implementations as recently as January 2020 with the Texas AuthentiCare implementation. The Account Manager becomes the post-implementation point of contact for change orders, enhancements, and defect resolution. See Proposal Section 3 for more detailed descriptions of these roles.

During Project Initiation and early in the Project Planning phases, FDGS works with DHHR to formalize the iterative Contract Milestones portrayed in the high-level timeline in Figure 4.4. The Contract Milestone approach monitors the progress by keeping track of milestones within each iteration and represent the best way to verify alignment at each milestone. Frequent contract milestones maintains alignment with requirements, allows for defects to be identified and corrected earlier, and provides the Department with demonstrations of the expanded AuthentiCare solution as more design, configuration, and testing is successfully completed.

Concluding each Contract Milestone is a demonstration of the updated AuthentiCare EVV application as more configuration is completed for the features and functions included in each cycle. This iterative approach provides for visibility to the changes and progression of development throughout the DDI phase while validating the functional system throughout. Preliminary Milestone dates begin six weeks after contract execution and every six weeks thereafter for three iterations. This schedule of three six-week iterations allows for changes to be grouped as is illustrated in the project plan.

Milestone demonstrations are used as a delivery vehicle for contract deliverables as well. As milestones are completed, the demonstrated business rules and deliverables are signed off by DHHR using a business rules matrix. Figure 4.2 portrays an example from a recent statewide implementation of how design and configuration items are tracked throughout the development phase and verified by the Department upon completion.

ID	Business Rule ID	Proposed Milestone	Demonstrated Milestone	Demonstrated Date	Business Rule ID	Business Requirement Statement	Validation/Approval Method	Success Criteria
1	PAO – 1	4	4	6/25/19	Vendor Selection	EVV Vendors are required to have received complete provider user profile information from Accenture/TMHP for each user before beginning onboarding process		
2	PAO – 2	3	3	6/4/19		EVV Vendors must contact provider users to review the onboarding process, expectations, and when required, schedule a time and date to install the EVV system.	Documentation	First Data will present the onboarding process flowchart.
3	PAO – 3	4	4	6/25/19	Provider user profile set-up and data elements validation	EVV system must create a unique profile in the EVV System for each provider user containing the identification information listed in PAO - 4 (at a minimum). This includes distinct profiles for contracted provider agencies and Financial Management Services Agencies (FMSAs), and CDS employers at a minimum.		
4	PAO – 4	3	4	6/25/19		EVV system must electronically document data elements for provider user identification information through the EVV Master Provider web service.	Demonstration	First Data will call the web service and then demonstrate the values returned in the web page.

Figure 4.2 – Sample business rule and deliverable tracking worksheet

Additionally, each milestone is prepared and executed based on a milestone checklist that is communicated prior to each demonstration to confirm that both DHHR and FDGS are aligned with the functionality to be demonstrated. The checklist is then used to confirm that all features and functions are included during the demonstration. Upon completion of milestones, a matrix is maintained in the file structure for all stakeholders to review that reflects when items were demonstrated and if the item passed the criteria for acceptance. Figure 4.3 displays a portion of an example from another recent statewide AuthentiCare milestone checklist for the features and functions to be demonstrated for User Onboarding.

Milestone	Section	Sub-Section	BR #	Description	Validation/Approval Method
MS2	User Onboarding	Service attendant profile set-up and data elements validation	PAO-8	EVV system must create a unique profile for each service attendant containing the service attendant identification information listed in PAO-9 (at a minimum). This includes agency employees.	Demonstration
MS2	User Onboarding	Service attendant profile set-up and data elements validation	PAO-10	EVV system must allow provider users with appropriate security access to initiate service attendant profile updates.	Demonstration
MS3	User Onboarding	Vendor Selection	PAO-2	EVV Vendors must contact provider users within required timeframes to review the onboarding process, expectations, and when required, schedule a time and date to install the EVV system.	Documentation
MS4	User Onboarding	Vendor Selection	PAO-1	EVV Vendors are required to have received complete provider user profile information from the SI Vendor for each user before beginning the onboarding process.	Demonstration
MS5	User Onboarding	Provider User profile set-up and data elements validation	PAO-3	EVV system must create a unique profile for each provider user containing the identification information from the EVV Master Provider web service. This includes distinct profiles for each type of provider user.	Demonstration
MS4	User Onboarding	Provider User profile set-up and data elements validation	PAO-4	EVV system must electronically document data elements for provider user identification information through the EVV Master Provider web service described in Appendix D.	Demonstration
MS4	User Onboarding	Provider User profile set-up and data elements validation	PAO-5	EVV system must validate identification data entered by provider user against the Data Aggregator using the EVV Master Provider web service. An error must be communicated to the user for any data elements that do not match and creation of provider user profile must not occur until the errors are corrected.	Demonstration

Figure 4.3 – Sample feature and function list captured for all contract milestone demonstrations

Identifying all enhancements and establishing backlog priorities up front allows the development iterations and all necessary documentation ample time to deliver a quality product on time. FDGS builds on past projects with a code base structure that is deployed in all jurisdictions, improving the customer experience. Due to the aggressive timeframe of the required six-month implementation period, all design documents will have to be expedited for approval by DHHR. FDGS will provide approval timelines to confirm that project schedules remain aligned with expected DHHR timelines. It is assumed that some requirements and enhancements to the

base product will be deferred to future phases as the scope of each phase is planned, documented, and approved.

Training will be provided for DHHR staff, providers, and other users, beginning in the Deployment Phase according to the agreed-upon Training and Outreach Plan. All translations, if requested through the Change Management process, will be completed after all training documents have been accepted by DHHR through a third-party translation service. Once the web and mobile user interfaces are completed and approved, FDGS will initiation the ADA accessibility verification and certifications through our third-party vendor.

File transfer for loading of providers, members, and authorizations, as well as transfer of claims and visit data to DHHR, will follow approved FDGS protocols.

Our approach to EVV services projects and high-level Gantt chart, shown in Figure 4.4, incorporates a proven project timeline and schedule that is designed to meet the planned six-month Go-Live target and subsequent transition to Maintenance and Operations. This proposed timeline provides a repeatable, high-level approach that we will tailor to your needs and adjust based on the final, agreed-upon contract dates and review periods between DHHR and FDGS.

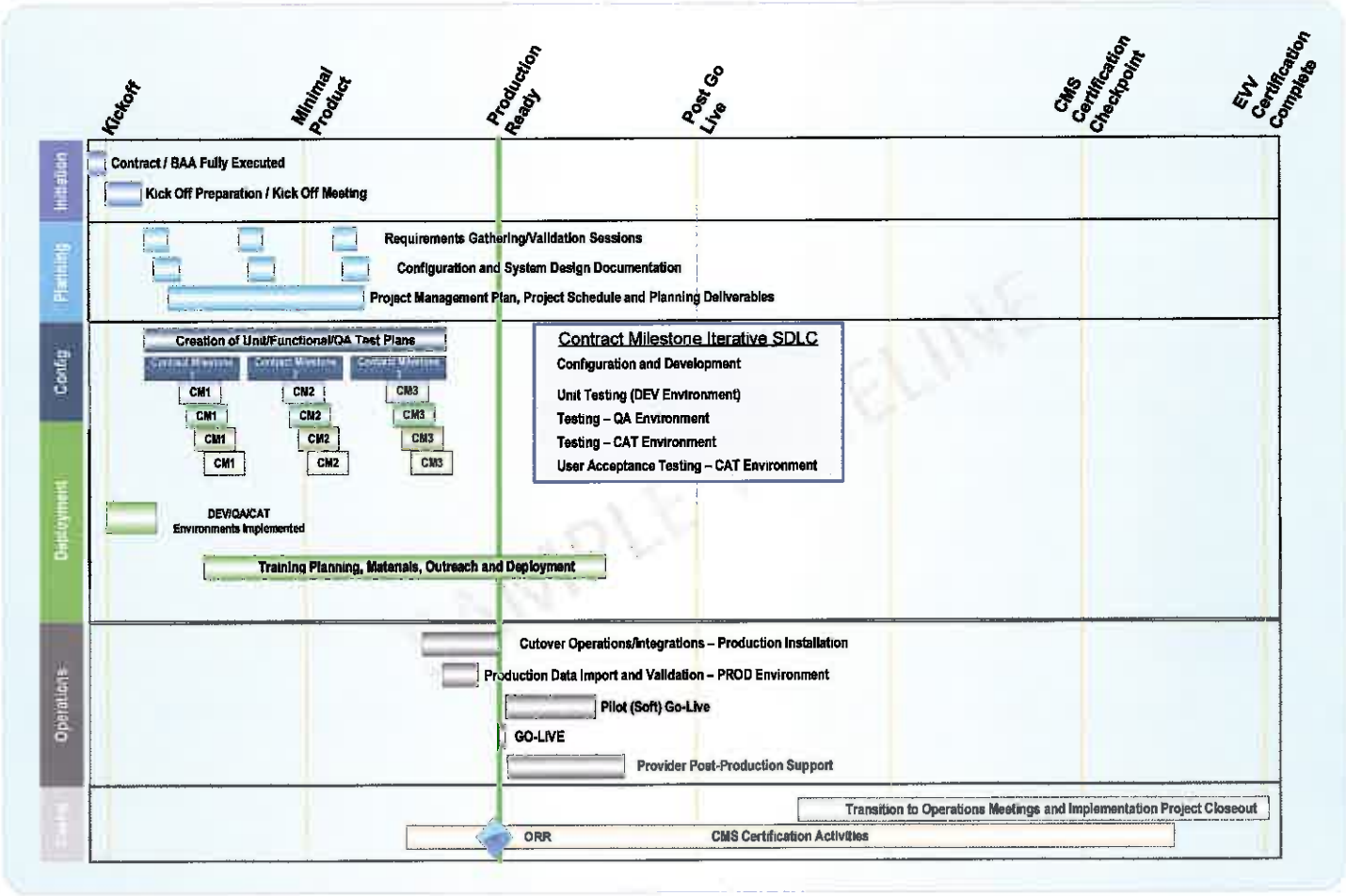


Figure 4.4 – AuthentiCare Implementation: High-Level Gantt Chart

We develop and maintain our draft project schedule using industry standard software. We base the Work Breakdown Structure (WBS) on the successful implementation of EVV systems in other states and MCOs with an iterative process for continuous improvement through lessons learned and internal training. We customize our baseline schedule to your specific RFP requirements and integrate it with the State's master work plan interdependencies where appropriate. At the end of this section, we include page images of our recommended approach to scheduling and accomplishing all tasks, activities, deliverables, and major milestones necessary to successfully implement the AuthentiCare EVV solution for the State of West Virginia.

Once approved, the schedule will be baselined within industry standard software and the Project Work Plan will follow a weekly update cycle to capture task, deliverable, milestone status, and approved changes, and feed the regular status meetings and status reports. FDGS understands the dynamic and "living" nature of the Project Work Plan. However, we will not re-baseline the schedule without formal approval from DHHR through the Change Management process. The Project Manager uses the information from this schedule to clearly and regularly communicate progress and potential risks to the DHHR project leadership and its stakeholders.

At the end of Proposal Section 4.1 Initial Work Plan Attachment, FDGS includes our draft of the Initial Work Plan for the DHHR EVV project. We will work with the Department to refine the schedule and finalize it for approval within the first month following the project kickoff meetings. As required by this RFP, we have also included the work plan as a separate tab.

4.1 Initial Work Plan Attachment

The initial work plan draft following this sub-section illustrates the detailed tasks and timelines while outlining the major project phases of how FDGS will meet the requirements for West Virginia's EVV solution. Once the deliverables are finalized with the Requirements Validation Sessions, FDGS will update the project work plan with updated durations and level of effort.

Our approach expedites the EVV implementation to quickly comply with the 21st Century Cures Act and prepare the Department for CMS Certification using the latest Outcomes-Based Certification guidance. This approach provides a fully functional EVV solution and maintains the maximum Federal Medical Assistance Percentage (FMAP) for the State.

4.1.1 Responsibilities

The FDGS Project Manager is responsible for the entire project work plan and its components. The Project Manager will work with DHHR to provide regular status according to the work plan.

Deliverable responsibilities will be finalized once the final list of deliverables is completed upon award. There are some deliverables that fall within existing AuthentiCare system documentation and others that do not apply for our hosted EVV solution. Based on the list of deliverables in the RFP (Cost Sheet Table 14 and Table 15), we have identified tentative owners for each deliverable in Table 4.1.

Once the deliverable list is finalized, each deliverable will then be assigned a clear owner and the appropriate business or technical analyst resources to complete each deliverable. Depending on the content of each deliverable, FDGS will work with the Department to also assign a primary point of contact for questions, clarifications, and reviews for each deliverable.

Table 4.1 – Tentative resource assignments by deliverable

Description		Resource Assigned
Task Group 1: Project Initiation and Project Management Plan		
Payment Milestone 1: Project Initiation Complete		
D001	Project Kickoff Meeting	Project Manager
D002	Change Management Plan	Project Manager
D003	Communication Management Plan	Project Manager
D004	Cost Management Plan	Project Manager
D005	Documentation Management Plan	Project Manager
D006	Modularity and Reusability Plan	Project Manager
D007	Project Work Plan	Project Manager
D008	Quality Management Plan	Project Manager
D009	Risk and Issue Management Plan	Project Manager
D010	Schedule Management Plan	Project Manager
D011	Scope Management Plan	Project Manager
D012	Staffing Management Plan	Project Manager
D013	Stakeholder Management Plan	Project Manager
Task Group 2: Solution Planning		
Payment Milestone 2: Solution Planning 1		
D014	Data Management Plan (including Governance and Quality)	Technical Lead
D015	Data Security, Privacy, and Confidentiality Plan	Technical Lead

D016	Incident Management Plan	Operations Manager
D017	Master Test Plan (Testing Management Plan)	Quality Manager
D018	Privacy Impact Analysis	Technical Lead
D019	Requirements Gap Analysis Document	Business/Technical Analyst
D020	Requirements Management Plan	Business/Technical Analyst
Payment Milestone 3: Solution Planning 2		
D021	Requirements Specification Document	Business/Technical Analyst
D022	Requirements Traceability Matrix	Business/Technical Analyst
D023	Safeguard Procedures Report	Technical Lead
D024	Security Plan	Technical Lead
D025	System Backup and Record Retention Plan	Technical Lead
D026	System Requirement Document/Backlog User Stories or Use Cases	Technical Lead
Task Group 3: Solution Design, Testing, and Operational Readiness		
Payment Milestone 4: Solution Design, Testing, and Operational Readiness 1		
D027	Capacity Plan	Technical Lead
D028	Configuration Management Plan	Technical Lead
D029	Data Conversion Plan	Business/Technical Analyst
D030	Data Conversion Test Cases	Quality Manager
D031	Data Conversion Test Results	Quality Manager
D032	Database Design Document and Data Models	Technical Lead
D033	Detailed System Design Document	Technical Lead
D034	Disaster Recovery and Business Continuity Plan	Operations Manager
Payment Milestone 5: Solution Design, Testing, and Operational Readiness 2		
D035	Federal Certification and Review Management Plan	Certification SME
D036	Interface Inventory	Business/Technical Analyst
D037	Load and Stress Test Cases	Quality Manager
D038	Load and Stress Test Results	Quality Manager
D039	Operational Readiness Plan	Certification SME
D040	Operational Readiness Test Scripts	Certification SME
D041	Operational Readiness Test Results	Certification SME
Payment Milestone 6: Solution Design, Testing, and Operational Readiness 3		
D042	Regression Test Cases	Quality Manager
D043	Regression Test Results	Quality Manager
D044	Reports and Forms Inventory	Business/Technical Analyst
D045	System Integration Plan	Technical Lead
D046	System Integration Test Cases	Quality Manager
D047	System Integration Test Results	Quality Manager
D048	Training Management Plan	Training Manager
D049	User Acceptance Test Cases	Quality Manager
D050	User Acceptance Test Results and Letter of Completion	Quality Manager
Task Group 4: Solution Deployment		
Payment Milestone 7: Deployment 1		
D051	Cutover Play Book	Technical Lead

D052	Federal Review Supporting Documentation	Certification SME
D053	Implementation Certification Letter	Certification SME
D054	Implementation Plan (Rollout Plan)	Technical Lead
D055	Operations Change Management Plan	Operations Manager
Payment Milestone 8: Deployment 2		
D056	Operational Milestone Review	Certification SME
D057	Product Screenshots, Reports, and Data Certification	Certification SME
D058	Report Distribution Schedule	Business/Technical Analyst
D059	Solution Health Monitoring Plan	Operations Manager
D060	System Operations Plan	Operations Manager
Payment Milestone 9: Deployment 3		
D061	System and User Documentation	Training Manager
D062	Training Materials	Training Manager
D063	Training Report	Training Manager
D064	Training Schedule	Training Manager
D065	Turnover and Closeout Management Plan	Project Manager
Task Group 5: Project Monitor & Control		
Payment - Monthly Implementation Project Management Invoice		
D066	Project Schedule	Project Manager
D067	Project Status Reporting (Weekly and Monthly)	Project Manager
D068	Risk Register/Exception Plan	Project Manager
D069	Updated Project Management Components	Project Manager
D070	Updated Requirements Traceability Matrix	Business/Technical Analyst
D071	Updated Training Management Plan	Training Manager

4.1.2 Timelines and Durations

The initial work plan below includes our initial estimates for the major phases from Project Kickoff to Go-Live, the Transition to Operations, and finally, post-implementation support for CMS certification activities. As the future phases are approved by the Department, the project work plan will be expanded by the FDGS Project Manager to establish a new baseline for tracking and reporting.

As part of our SDLC, we include several iterative cycles for design, configuration, and testing that we call Contract Milestones. For the six-month implementation period requested by the Department in this RFP, we have estimated three unique Contract Milestones. At the conclusion of each milestone, FDGS will provide a demonstration of the features and functions included in each cycle (building upon the prior cycle). We have found that this approach helps the Department and its stakeholders to see the progress of the EVV project and provide immediate feedback during and following the demonstration.

In addition to AuthentiCare's major SDLC phases, we have included the Payment Milestones to align the RFP's payment milestones, task groups, and deliverables within our project schedule.

4.1.3 Milestone Dates

Some key milestone dates have been included in the initial work plan such as the Go-Live date targeted six months following the start of the project. Additional milestones will be added based on the contract negotiation and project kickoff activities.

4.1.4 Deliverable Dates

FDGS has aligned the Task Groups with our major SDLC phases. Some deliverables will be completed as part of our normal system documentation. For example, our System Implementation Plan (SIP) includes much of the documentation necessary for the Department to understand the components of AuthentiCare and how they are deployed to support the West Virginia EVV solution. We maintain a baseline SIP that aligns to the base AuthentiCare product. We are able to modify the SIP based on unique configurations, business rules, and workflows necessary to implement AuthentiCare in West Virginia.

Once the final list of deliverables is approved, the FDGS Project Manager will update the Project Work Plan to include the deliverables and the planned completion dates.

4.1.5 Vendor personnel hours by deliverables for each project phase

As the final list of deliverables is approved, we assign resources from our business and technical resource pools to complete each deliverable by the agreed upon due dates to maintain the integrity of the overall schedule. FDGS can add personnel from our different resource pools to specific deliverables as needed to keep the work plan dates intact.

4.1.6 Department of Health and Human Resources (DHHR) personnel hours by phase deliverable

The focus of DHHR personnel by phase will be updated iteratively as the project approaches each phase. The focus will be on deliverable reviews and walkthroughs. We have found that participation in interactive walkthroughs deepens the understanding with the Department personnel and expedites the review and approval process to keep hours to a minimum.

Within each phase, the FDGS Project Manager will communicate the upcoming deliverables that will require DHHR personnel to participate in design sessions, documentation reviews, deliverable walkthroughs, and support final approval of their respective deliverables.

4.1.7 All critical dependencies for the project's milestones and deliverables

With our iterative cycles (Contract Milestones) included in the initial work plan, we are able to conduct overlapping activities from one cycle to the next. This minimizes the number of critical dependencies across the initial phase and the move to production. During the project kickoff meetings and other project start-up activities, the FDGS team will work directly with the Department and its stakeholders to further identify external dependencies, additional project risks or issues, and greater view into the Department's Medicaid enterprise.

For example, in other states, we have integrated critical dependencies related to interfacing with the MMIS system due to enhancements already in progress. We will work with the different technical resources on the state side as well to determine if interface or integration testing may pose dependencies that could affect the final work plan.

4.1.8 Prompt DHHR Acceptance

With an aggressive six-month implementation period, we know that extended review and approval cycles for more than 50 deliverables is a significant risk to meeting the Department's goals in complying with the 21st Century Cures Act and readiness for CMS certification of the EVV system. FDGS will work with the Department to properly prepare and plan for expedited reviews and approvals of the deliverables.

At a minimum, the FDGS Project Manager will verify all deliverables that are currently planned for review or approval within the upcoming 45 days with the Department. These will also be included in the regular status reports.

AuthentiCare West Virginia Department of Health and Human Resources (DHHR) - EVV Project Schedule (Draft)

ID	Outline Number	Task Name	Duration	Start	Finish	Predecessors	Resource Names
0	0	*WV EVV - AuthentiCare Implementation*	*282 days*	*6/1/20*	*6/30/21*		
1	1	**Contract Award (Pre-Project)**	**20 days**	**6/1/20**	**6/26/20**		
2	1.1	Contract Award Milestone	0 days	6/1/20	6/1/20		
3	1.2	Contract Negotiation (assumed to be 4 weeks)	20 days	6/1/20	6/26/20	2	
4	1.3	MILESTONE: Contract and BAA - Fully Executed	0 days	6/26/20	6/26/20	3	
5	2	**Project Initiation**	**4 days**	**6/26/20**	**7/1/20**		
6	2.1	MILESTONE: DAY ONE - Project Start	0 days	7/1/20	7/1/20	4	
7	2.2	Prepare for Project Kickoff Meeting	2 days	7/1/20	7/2/20	4	PM
8	2.3	Project Kick Off Meetings with DHHR	2 days	7/6/20	7/7/20	7	PM
9	2.4	Document Kickoff Outcomes and Distribute	1 day	7/8/20	7/8/20	8	PM
10	3	**Planning, Administration, and Detailed Design**	**59 days**	**7/1/20**	**9/22/20**		
11	3.1	**Project Management Plans**	**11 days**	**7/1/20**	**7/16/20**	9	
12	3.1.1	**Project Work Plan**	**6 days**	**7/6/20**	**7/13/20**	4	
13	3.2	Onsite Requirements Gathering and Clarifications	3 days	7/9/20	7/13/20	9	
14	3.3	Requirements Traceability Matrix (RTM)	3 days	7/9/20	7/13/20	9	
15	3.4	**Detailed System Design (DSD) Documentation**	**52 days**	**7/13/20**	**9/22/20**	13,14	BA,SME,DHHR
16	3.4.1	**System Integration Plan (SIP)**	10 days	7/14/20	7/27/20	13,14	BA,SME,DHHR
17	3.4.2	**Import Specifications - Appendix B**	13 days	7/14/20	7/30/20	13,14	BA,SME
18	3.4.3	**WV Specifications Document**	13 days	7/14/20	7/30/20	13,14	BA,SME
19	3.4.4	**Web Services - Appendix S**	13 days	7/14/20	7/30/20	13,14	BA,SME
20	3.4.5	**Overall IVR Architecture and Flow - Appendix C**	5 days	7/14/20	7/20/20	13,14	BA,SME
21	3.4.6	**Mobile - Appendix W**	18 days	7/14/20	8/6/20	13,14	
22	3.4.7	**Compliance Reviews**	7 days	7/29/20	8/6/20	21FF	
23	4	*Task Group 1 Deliverables - Project Initiation and Project Management Task Gro*	1 day	9/23/20	9/23/20	15	PM,DHHR
24	6	**Config/Deployment**	**108 days**	**8/3/20**	**12/30/20**		
25	5.1	**Iteration 1 Config and Dev (C1)**	**30 days**	**8/3/20**	**9/11/20**		
26	5.1.1	**Configuration and Design Documentation**	**2 days**	**8/3/20**	**8/4/20**		
27	5.1.1.1	Milestone #1 - System Integration Plan Design Acceptance	2 days	8/3/20	8/4/20	16	DHHR,FD
28	5.1.1.2	Milestone #2 - Publish Test Cases & Scripts	2 days	8/3/20	8/4/20	27FF	DHHR,FD
29	5.1.1.3	Milestone #3 - Configuration and Design Document Acceptance	2 days	8/3/20	8/4/20	28FF	DHHR
30	5.1.2	**Development**	**20 days**	**8/5/20**	**9/1/20**		
31	5.1.2.1	Milestone #4 - Set Up Environments	2 days	8/5/20	8/6/20	29	FD
32	5.1.2.2	Milestone #5 - Set Up and Configure IVR	2 days	8/5/20	8/6/20		FD
33	5.1.2.3	Milestone #6 - Development Complete (Unit)	20 days	8/5/20	9/1/20		
34	5.1.3	**Testing (Team Testing)**	**8 days**	**9/2/20**	**9/11/20**		
35	5.1.3.1	Milestone #7 - Product Testing Complete (QA and CAT)	3 days	9/2/20	9/4/20	33	FD
36	5.1.3.2	Milestone #8 - User Acceptance Testing Complete	6 days	9/4/20	9/11/20	35FF	DHHR
37	5.1.4	Contract Milestone (C1)	1 day	9/11/20	9/11/20	34FF	DHHR,PM
38	5.1.5	*Task Group 2 Deliverables - Solution Planning*	1 day	9/11/20	9/11/20	37FF	PM,DHHR
39	5.2	**Iteration 2 Config and Dev (C2)**	**36 days**	**9/11/20**	**10/30/20**		
40	5.2.1	**Configuration and Design Documentation**	**2 days**	**9/11/20**	**9/14/20**		
41	5.2.1.1	Milestone #1 - Update System Integration Plan	2 days	9/11/20	9/14/20		DHHR,FD
42	5.2.1.2	Milestone #2 - Update Test Cases & Scripts	2 days	9/11/20	9/14/20	41FF	DHHR,FD

AuthentiCare West Virginia Department of Health and Human Resources (DHHR) - EVV Project Schedule (Draft)

ID	Outline Number	Task Name	Duration	Start	Finish	Predecessors	Resource Names
43	5.2.1.3	Milestone #3: Configuration and Design Document Acceptance	2 days	9/11/20	9/14/20	42FF	DHHR
44	5.2.2	**Development**	**26 days**	**9/11/20**	**10/16/20**		
45	5.2.2.1	Milestone #4 - Update Environments	2 days	9/11/20	9/14/20		
46	5.2.2.2	Milestone #5 - Update IVR	2 days	9/11/20	9/14/20		
47	5.2.2.3	Milestone #6 - Development Complete (Unit)	25 days	9/11/20	10/15/20		
48	5.2.3	**Testing (Team Testing)**	**11 days**	**10/16/20**	**10/29/20**		
49	5.2.3.1	Milestone #7 - Product Testing Complete (QA and CAT)	5 days	10/16/20	10/22/20	47	FD
50	5.2.3.2	Milestone #8 - User Acceptance Testing Complete	6 days	10/23/20	10/30/20	49	DHHR
51	5.2.4	Contract Milestone (C2)	1 day	10/30/20	10/30/20	48FF	DHHR,PM
52	6	**Scaled WV AuthentiCare Model Go-Live**	**43 days**	**11/2/20**	**12/30/20**		**Dev team\PM**
53	6.1	Select and Onboard Providers of different sizes	5 days	11/3/20	11/9/20	50	DHHR,FD
54	7	**Iteration 3 Config and Dev (C3)**	**43 days**	**11/2/20**	**12/30/20**		
55	7.1	**Configuration and Design Documentation**	**2 days**	**11/2/20**	**11/3/20**		
56	7.1.1	Milestone #1 - Update System Integration Plan	2 days	11/2/20	11/3/20		
57	7.1.2	Milestone #2 - Update Test Cases & Scripts	2 days	11/2/20	11/3/20	56FF	
58	7.1.3	Milestone #3 - Configuration and Design Document Acceptance	2 days	11/2/20	11/3/20	57FF	
59	7.2	**Development**	**30 days**	**11/3/20**	**12/14/20**		
60	7.2.1	Milestone #4 - Update Environments	2 days	11/3/20	11/4/20		
61	7.2.2	Milestone #5 - Update IVR	2 days	11/3/20	11/4/20		
62	7.2.3	Milestone #6 - Development Complete (Unit)	30 days	11/3/20	12/14/20		
63	7.3	**Testing (Team Testing)**	**13 days**	**12/14/20**	**12/30/20**		
64	7.3.1	Milestone #7 - Product Testing Complete (QA and CAT)	6 days	12/14/20	12/21/20		
65	7.3.2	Milestone #8 - User Acceptance Testing Complete	6 days	12/21/20	12/28/20	64FF	
66	7.4	ADA Validation Provided from Vendor	1 day	12/29/20	12/29/20	65	FD
67	7.5	Contract Milestone (C3)	1 day	12/30/20	12/30/20	63FF	DHHR,PM
68	8	**ORR Preparation**	**43 days**	**11/2/20**	**12/30/20**		
69	8.1	Validate scripts for evidence	5 days	11/16/20	11/20/20	44	FD CMS SME
70	8.2	Schedule 3rd party audit functions and reports	5 days	11/2/20	11/6/20	39	FD CMS SME
71	8.3	Criteria Evidence 1 - 10 generate and reviews	10 days	11/16/20	11/27/20	48SF+10 days	FD CMS SME
72	8.4	Criteria Security 1 Auditor Summary Report	2 days	12/3/20	12/4/20	71SF+15 days	FD CMS SME
73	8.5	Submit Evidence for scheduled ORR	1 day	12/4/20	12/4/20	72FF	FD CMS SME
74	8.6	Conduct Operational Readiness Review (ORR) with DHHR and CMS (TBD)	1 day	12/21/20	12/21/20	73	DHHR,FD CMS SI
75	9	**Operational/Helpdesk Activities**	**8 days**	**12/21/20**	**12/30/20**		
76	9.1	Phone number Helpdesk Set Up	1 day	12/21/20	12/21/20		
77	9.2	Monthly Reporting	8 days	12/21/20	12/30/20		
78	9.3	Training of Helpdesk Staff	1 day	12/22/20	12/22/20		Training Lead
79	10	**Training and Outreach Activities**	**193 days**	**7/1/20**	**3/29/21**		**Training Lead**
80	10.1	Training and Outreach Plan	57 days	7/1/20	9/18/20		Training Lead
81	10.2	Training	82 days	12/8/20	3/31/21		Training Lead
82	11	*Task Group 3 Deliverables - Solution Design, Testing, and Operational Readines*	1 day	2/26/21	2/26/21		DHHR,PM
83	12	**AuthentiCare Go/No Go Decision**	**9 days**	**12/21/20**	**12/31/20**		
84	12.1	Perform AuthentiCare Go/No Go Assessment After ORR	9 days	12/21/20	12/31/20		DHHR,FD
85	13	**Operations & Maintenance (Production Readiness)**	**60 days**	**1/4/21**	**3/26/21**		

AuthentiCare West Virginia Department of Health and Human Resources (DHHR) - EVV Project Schedule (Draft)

ID	Outline Number	Task Name	Duration	Start	Finish	Predecessors	Resource Names
86	13.1	Post Go Live Production Data Validation/Testing	5 days	1/4/21	1/8/21		
87	13.2	MILESTONE: Go Live Begins	0 days	1/4/21	1/4/21		
88	13.3	*Production Roll Out*	*65 days*	*1/4/21*	*4/2/21*	*87*	
89	**13.4**	**Cutover - Go-Live**	**1 day**	**1/4/21**	**1/4/21**	**88**	
90	**13.5**	**Go-Live Support**	**20 days**	**1/4/21**	**1/29/21**		
91	14	*Task Group 4 Deliverables - Solution Deployment*	1 day	1/4/21	1/4/21	89FF	DHHR,PM
92	**15**	**Closeout**	**60 days**	**1/4/21**	**3/26/21**		
93	15.1	Provide Transition Documention	10 days	1/4/21	1/15/21		FD
94	**15.2**	**Closeout Implementation and Transition to M&O Plan**	**6 days**	**1/4/21**	**1/11/21**		
95	15.3	Conduct a Transition to M&O Meeting	1 day	1/18/21	1/18/21	93	FD,DHHR
96	15.4	Conduct Implementation Project Close Out Meeting	1 day	1/19/21	1/19/21	95	FD,DHHR
97	15.5	**Implementation Project Closeout and Lessons Learned Report**	7 days	1/20/21	1/28/21	96	
98	16	*Task Group 5 Deliverables - Project Monitor and Control*	1 day	1/29/21	1/29/21		DHHR,PM
99	**17**	**Post-Implementation CMS Certification Support (Schedule TBD)**	**128 days**	**1/4/21**	**6/30/21**		
100	17.1	Provide Evidence for Post Go Live CMS Certification Requirements (TBD)	65 days	4/1/21	6/30/21	87	FD CMS SME
101	17.2	Continued Support through Stabilization Period (Duration - TBD)	128 days	1/4/21	6/30/21		FD CMS SME
102	17.3	MILESTONE: CMS Final Milestone Review Certification (TBD)	0 days	6/30/21	6/30/21	101	FD CMS SME,WD

4.2 Abridged Project Management Plan

The FDGS Project Management Plan (PMP) is ready to be expanded with specific details required for the West Virginia EVV project. The full PMP includes management and administrative details to clearly maintain document control and structure information including:

- Document History
- Document Control
- Project Deliverable Sign-off
- Table of Contents

For the abridged version, we have included introductions to each sub-plan of our PMP. The PMP for the AuthentiCare EVV project may include the following chapters:

1.0 Introduction

2.0 Assumptions, Constraints, and Risks

3.0 Scope Statement

4.0 Project Work Plan and Schedule

5.0 Entrance and Exit Criteria

6.0 Quality Milestone Review

7.0 Project Documentation Management

8.0 Resource Management Plan

9.0 FDGS Project Team Organizational Chart

10.0 Communication Plan

11.0 Risk Management Plan

12.0 Issue Management Plan

13.0 Quality Management Plan

14.0 Change Management Plan

4.2.1 Introduction

This Project Management Plan (PMP) provides a draft of the detailed plans, processes, and procedures for managing and controlling the life cycle activities of the West Virginia Electronic Visit Verification (EVV) Project. It includes a set of project management tools, processes, and procedures that both the FDGS and Department project teams will use to help confirm efficient project operations and that sets the standard for quality work products and deliverables.

The Introduction includes:

- Department Goals and Objectives
- FDGS Project Goals and Objectives
- Acronyms and Terms

4.2.2 Assumptions, Constraints, and Risks

FDGS will initially populate known Assumptions, Constraints, and Risks during the initiation phase of the project and continue to expand this section as the project progresses through each implementation phase and Go-Live.

4.2.3 Scope Statement

FDGS will update the project Scope Statement. The following is a sample scope statement.

West Virginia Department of Health and Human Resources (DHHR) will implement a centralized, web-based Electronic Visit Verification (EVV) solution for Personal Care Services (PCS) and Home and Community Based Services (HCBS) to prevent inappropriate billing/payment, safeguard against fraud, improve program oversight, and enhance quality of services. The State will deploy a vendor-hosted application to serve as the State's EVV solution in compliance with the 21st Century Cures Act.

4.2.4 Project Work Plan and Schedule

This subsection of the FDGS PMP first provides a schedule overview to portray the integrated phases of our plan. Following the overview, we include the full detail of the initial EVV Project Work Plan containing our recommended approach to scheduling in order to accomplish all tasks and activities identified within this RFP.

4.2.5 Entrance and Exit Criteria

FDGS uses the industry's best practices and standards to develop the entrance and exit criteria for each project phase, requiring customer approval before initiation of subsequent phases in a waterfall or hybrid project. However, even both waterfall and hybrid project lifecycles can benefit from some flexibility in the Phase Entrance and Exit criteria. FDGS will work with the Department to establish specific entrance and exit criteria for progressing through the project phases. The criteria will control entrance and exit to the Configuration, Deployment, and Operations and Maintenance phases. The entrance and exit criteria must be approved by the Department prior to proceeding beyond the Planning and Administration Task.

4.2.6 Quality Milestone Review

The Quality Milestone review is an opportunity for the management team to review the program progress, assess the program's total health, and decide on the next steps. The project milestones are a gate that can be passed once the deliverables and tasks represented by the milestone are completed. The deliverables within the milestone are assessed to determine the overall health of the milestone.

We use the "stoplight" method for noting the status of each milestone, assessing a value of green, yellow, or red for each deliverable at each milestone:

- Green indicates the team has fully met the criteria for the deliverable
- Yellow indicates the team has not fully met the criteria but has a work plan to achieve the criteria
- Red indicates the team has not fully met the criteria and has no plan developed to meet the criteria (requiring intervention from management)

The milestone is approved if the metrics are green for all the deliverables at the milestone. There are situations when the approval is given even though there are unresolved issues. In this case, the program team is tasked with resolving the open issues at a later time.

The milestone progress is reported to the management team on the weekly project status report and as needed throughout the project to validate the overall health of the project.

4.2.7 Project Documentation Management

FDGS will provide the project management tools for the AuthentiCare team to successfully accomplish all EVV project tasks and create the required deliverables. We use software familiar to most users to enhance productivity, promote collaboration, and minimize barriers to participation. However, as part of the initial planning process, and as needed throughout the project, we review software preferences and user accessibility needs to confirm we are meeting the Department's needs.

- FDGS develops most of the project deliverables, meeting agendas, and meeting minutes using industry standard software tools.
- FDGS uses industry standard software tools to develop and maintain project schedules and work plans. Where licensing constraints present a barrier, FDGS can easily provide alternative formats such as PDF files for ease of access.
- FDGS uses industry standard software tools primarily for communicating key information during presentations and training sessions. In addition to displaying presentations on a display screen, we provide hard copies of the presentation for participants. This is also a tool we use for presenting information to Executive Management or external stakeholders. FDGS can easily provide alternative formats such as PDF files for ease of access.
- FDGS uses industry standard software tools for developing organization charts, flowcharts, and business process diagrams. FDGS can easily provide alternative formats like PDF files for ease of access.
- FDGS uses industry standard software tools for document management and process documentation for all of our projects.

FDGS will evaluate all project documentation and deliverables to tailor appropriately according to the Department's document standards.

Additional details for this section include:

- Document Management Procedures
- Document Naming Conventions

4.2.8 Resource Management Plan

One of the keys to success for any project is the team. This plan addresses the approach that helps enable staff to succeed in their project assignments. This plan encompasses both FDGS and Department resources associated with the EVV Project. FDGS will work with the Department to refine the resource plan as required for the EVV Project.

To clearly define project roles, this section will detail the responsibilities of each role. If additional clarification is needed, an expanded RACI matrix may also be included to further define responsibilities.

4.2.9 FDGS Project Team Organizational Chart

Along with the diagram of the current organizational chart, this section will include additional details regarding the staffing or resource management plan including:

- Staff Management
- Key Personnel
- Staff Transition (replacement and roll-off)
- Personnel/Performance Issues

4.2.10 Communication Plan

The Communication Plan identifies the formal communication approach, processes, procedures, and protocols that will be employed to keep all project stakeholders informed throughout the duration of the EVV project. The FDGS Project Manager will work with the Department's leadership and stakeholders to refine the Communication Plan as needed for the EVV project.

This sub-plan is one of the most important and may be updated more often than the others as project needs change. This section includes the various communication methods and media that will be used to clearly communicate to the different stakeholder groups. The communication matrix is included to clearly list the information supporting the development of internal and external messaging.

Table 4.2 describes the planned communications for the West Virginia EVV Project. The table identifies the intended audience, the item, and the frequency, format, and method of delivery. Standard formats will be applied to all documents to provide consistency.

Table 4.2 – Project Communication Methods

Communication Item	Owner	Description	Audience	Frequency	Method/ Media
Meeting Agendas	FDGS	Meeting topics, logistics	Meeting Attendees	Minimum 24 hours prior to meeting	Document distributed via email and as meeting handout
Meeting Minutes	DHHR/ FDGS	High-level verbal agreements and action items	Meeting Attendees	Within five business days after meeting	Document distributed via email
Status Report	FDGS	These status reports detail accomplishments for the reporting period, planned activities for the next reporting period, any progress, and/or anomalies versus the approved Work Plan, new issues and/or risks identified, and an updated status on existing issues and risks.	Primary: DHHR Secondary: Other Project Stakeholders	Weekly, Bi-Weekly, Monthly *As required by project phase	Document distributed via email

Communication Item	Owner	Description	Audience	Frequency	Method/ Media
Work Plan/Schedule	FDGS	Project Schedule of Tasks, Duration, Milestones	Primary: DHHR Secondary: Other Project Stakeholders	As needed, no less than monthly	Schedule distributed via email
Risk Register	FDGS	Summary list of potential project problems, and associated remediation and status	Primary: DHHR Secondary: Other Project Stakeholders	Monthly	Workbook distributed via email
Issue Log	FDGS	Summary list of project concerns or needs, and associated status	Primary: DHHR Secondary: Other Project Stakeholders	Monthly	Workbook distributed via email
Deliverable Approval Forms	FDGS	Request formal approval of final deliverables	Primary: DHHR Secondary: Other Project Stakeholders	As needed	Sign-off form distributed via email
FDGS Deliverable Log	FDGS	Status of current and past FDGS deliverables	Primary: DHHR Secondary: Other Project Stakeholders	Monthly	Workbook distributed via email
Change Order Form	DHHR/ FDGS	Formal approval to changes to project scope, schedule, and cost.	DHHR	As needed	Document distributed via email, stored on project LAN or Project Website
Change Order Matrix	FDGS	Status on current and past Change Order Forms	DHHR	As needed	Document distributed via email

In addition, the Communication Plan includes:

- Communication Roles and Responsibilities
- Communication Tracking and Storage
- Communication Format
- Measuring Communication Effectiveness
- Communication Changes
- Communication Management Matrix (table)

4.2.11 Risk Management Plan

The Risk Management Plan documents the approach and procedures used to manage risk associated with the EVV project. Internally, FDGS uses its project tracking tool for the management and tracking of all risks related to a project. The team also maintains a customer-facing version of the risk and issue log for all action items, issues, and risks. The log is formatted in a workbook and reviewed during the regular status meetings. If preferred, risks may be tracked within a tool provided by the Department.

The Risk Management Plan can be broadly mapped into the six steps. Each step is described in detail throughout the remainder of the full Risk Management Plan.

A risk is any factor that may potentially interfere with the scope, schedule, cost, or quality of the project; it is the recognition that a problem or opportunity might occur. FDGS will work with the Department to review and tailor the Risk Management workflow for the EVV project. The FDGS Project Manager will provide updates of the most critical risks in regular status meetings and in written status reports.

We will categorize risks that may impact the project using the categories listed in Table 4.3 – Risk Categories below. Each category represents a common source or risk for the business or application area. Because we are familiar with issues that commonly become project risks, we know how to effectively mitigate risks or convert them into project opportunities.

Table 4.3 – Risk Categories

Risk Category	Examples
Technical	• Reliance on untested or complex technology • Unrealistic performance goals • Changes to the proposed technology • Integration with existing systems • Changes to industry standards during the project
Schedule	• Project team's ability to meet deliverable dates based on scope changes or resource availability • Overall accuracy of the proposed schedule
Cost	• Additional costs for additional staff or staff turnover • Changes to project approach that call for additional resources • Solving problems in design, application, or operations • Cost-related risks are often linked to schedule risks
Project Management	• Poor allocation of time or resources • Low-quality project plan • Lack of robust project management practices
Quality	• Lack of resources allocated to quality assurance tasks • Poorly defined standards and methodology
Organizational	• Internally inconsistent cost, schedule, or scope objectives • Poorly defined priorities • Inadequate or interrupted funding • Resource conflicts with other projects in the organization
External	• Shifting legal or regulatory environment • Labor issues • Changing state or federal priorities • Vendor contract issues

This section is extensively detailed as follows:

- Roles and Responsibilities (Risk Management)
- Risk Management Tool Procedures

- Risk Identification
  - Risk Categories
  - Risk Assignment
  - Risk Identification Outputs
- Risk Analysis Approach
  - Probability
  - Impact
  - Timeframe
  - Exposure
  - Prioritization
- Risk Response Planning
  - Risk Response Strategy
  - Risk Response Outputs
- Risk Monitoring and Controlling
  - Report Risk Status
  - Close Risks
  - Risk Monitoring and Controlling Outputs
- Risk Communication
- Risk Escalation Process

4.2.12 Issue Management Plan

The Issue Management Plan documents the approach, procedures, tasks, and tools that FDGS uses to manage issues associated with the EVV project. The purpose of issue management is to help provide proper oversight and management of issues that arise throughout the project. FDGS uses its project tracking tool for the managing and tracking all issues related to a project. The team also maintains a customer-facing version of the risk and issue log for all action items, issues, and risks. The log is formatted and reviewed during the regular status meetings. If preferred, issues may be tracked within a tool provided by the Department.

An issue is a statement of concern or need that:

- Is known ahead of time or contained in the project work plan, but whose resolution is in question or lacking agreement among stakeholders
- Is highly visible or involves external stakeholders
- Relates to a critical deadline or timeframe
- Results in an important decision or resolution whose rationale and activities must be captured for historical purposes
- If not resolved, may impede project progress

An issue is a situation that has occurred—as opposed to a risk, which is a potential event. Items that are "normal" day-to-day tasks related to a person's normal job duties are not considered issues.

Similar to the Risk Management Plan, the draft Issue Management Plan assumes coordination and reporting through the FDGS Project Manager and team members. During project initiation, FDGS will work with the Department to provide the updated Issue Management Plan, designating and assigning FDGS roles specific to the EVV project and issue management.

The issue management process consists of the steps listed below, which are described in the following subsections Issue Identification and Documentation:

- Identification/Documentation
- Validation, Assignment, and Prioritization
- Analysis
- Tracking and Reporting
- Issue Escalation Process
- Resolution and Closure

4.2.13 Quality Management Plan

The purpose of the Quality Management function is to verify that the EVV project objectives are met and the expected results are achieved via the quality-driven processes. These objectives will be achieved by defining quality assurance (QA) standards, core processes, and work products that will be used to manage quality throughout the lifecycle of the project.

The Quality Assurance Management Plan is a guideline for incorporating QA and quality control (QC) processes into all aspects of the EVV project. The QA Management Plan delineates the approach, processes, and set of checkpoints necessary to monitor the EVV project. Quality activities are used to verify that the EVV project will deliver on:

- **Business Goals**: Meeting Department expectations and safeguarding client satisfaction by understanding how the Department defines success
- **Quality Goals**: Minimizing errors and re-work by verifying and validating the work at each stage
- **Implementation Goals**: Improving speed, quality, and cost of delivery by assessing and improving the EVV project processes and procedures

During project initiation, FDGS will work with the Department to confirm the QA Management Plan designates and assigns all appropriate QA and Administrative positions that are specific to the EVV project. Additional documentation of the approach to quality include:

- QA/QC Roles and Responsibilities
- Quality Management Objectives
- Quality Assurance Checkpoints

4.2.14 Change Management Plan

The purpose of the Change Management Plan is to confirm that any changes occurring within the project are promptly identified, coordinated, and agreed upon, and properly managed. FDGS understands that change is inevitable in any project of this size. In an effort to verify that changes will not have a negative impact on project success, in terms of scheduled completion, budgetary constraints, quality, or customer satisfaction, changes to plans should be expected and addressed systematically. The Change Management Plan encompasses modifications to any of the following key areas:

- **Scope**: Agreed-upon features and functions of a product or service being produced by the project, and all related requirements and deliverables
- **Project Work Plan/Schedule**: Including the Project Work Plan, planned task sequencing, task start and end dates, resource plan, baseline schedule, and baseline costs
- **Project Management Plans**: Including the resource plan, communication, risk, and issue management plans, quality management plan, and change management plan
- **Issues**: Process developed to monitor and manage issues since issues have the potential to become changes

In our experience, changes tend to be viewed from a negative perspective, especially those that extend the schedule or result in additional costs; however, FDGS focuses on an approach that identifies changes that could benefit the project. FDGS will also work to identify neutral changes, including "trade-offs" or exchanging one item for another.

Given the importance and visibility of the EVV project, it is imperative that executive leadership, including Department sponsors, take an active role in the change process. FDGS assumes that the Department sponsors will be the approval authority for formal changes to the EVV project. FDGS and the Department will collaborate to determine which project participants should be involved for different types of changes.

FDGS assumes that when changes affect the project schedule, cause an increase in the project budget, or require change orders/contract amendments, Department sponsors will want to be more engaged in the process. When changes do not affect the schedule, budget, scope, or contracts, FDGS assumes that our team will assume primary responsibility for addressing and implementing such changes.

4.2.15 Stakeholder Management Plan

The Stakeholder Management Plan is a key part of setting the West Virginia EVV project on the right track early and maintaining a focus on project objectives. Stakeholders are any person or organization that can influence the project's outcome or who will be impacted by the project. Identifying stakeholders and working with them throughout the project helps the project team to stay on task and confirm that it is serving the parties most affected by the EVV project.

As part of the Stakeholder Management Plan, establishing a stakeholder engagement strategy early identifies the stakeholders from the various user groups. Next, FDGS analyzes the stakeholders to determine what level of impact, influence, and interest they have in the project and its objectives. Then, FDGS develops strategies for keeping stakeholders engaged, based on each stakeholder's unique needs and goals.

As the Stakeholder Management Plan is expanded FDGS will examine the following sub-sections of the plan based on our experience and lessons learned from other EVV projects:

- **Roles and Responsibilities**: FDGS will work with the Department to identify and confirm staff that will support stakeholder management throughout the duration of the implementation phase and into M&O.
- **Stakeholder Identification**: FDGS will work with the Department to validate the key user groups, stakeholders from the state and provider agencies, important project sponsors, and other user groups that may influence the EVV project.
- **Stakeholder Analysis**: After identifying project stakeholders, FDGS analyzes stakeholders to identify their interests, methods of influence, and potential risks. We also consider which individuals are critical to project success and which could adversely impact the project.
- **Stakeholder Management Strategies**: FDGS determines how best to manage each stakeholder to achieve project goals, including the method and frequency of communication, and the type of messaging that is most effective for each stakeholder or user group.
- **Stakeholder Register**: The Stakeholder Register is a repository of all information for people and organizations associated with West Virginia EVV project.

AuthentiCare West Virginia Department of Health and Human Resources (DHHR) - EVV Project Schedule (Draft)

ID	Outline Number	Task Name	Duration	Start	Finish	Predecessors	Resource Names
0	0	*WV EVV - AuthentiCare Implementation*	*282 days*	*6/1/20*	*6/30/21*		
1	1	**Contract Award (Pre-Project)**	**20 days**	**6/1/20**	**6/26/20**		
2	1.1	Contract Award Milestone	0 days	6/1/20	6/1/20		
3	1.2	Contract Negotiation (assumed to be 4 weeks)	20 days	6/1/20	6/26/20	2	
4	1.3	MILESTONE: Contract and BAA - Fully Executed	0 days	6/26/20	6/26/20	3	
5	2	**Project Initiation**	**4 days**	**6/26/20**	**7/1/20**		
6	2.1	MILESTONE: DAY ONE - Project Start	0 days	7/1/20	7/1/20	4	
7	2.2	Prepare for Project Kickoff Meeting	2 days	7/1/20	7/2/20	4	PM
8	2.3	Project Kick Off Meetings with DHHR	2 days	7/6/20	7/7/20	7	PM
9	2.4	Document Kickoff Outcomes and Distribute	1 day	7/8/20	7/8/20	8	PM
10	3	**Planning, Administration, and Detailed Design**	**59 days**	**7/1/20**	**9/22/20**		
11	3.1	**Project Management Plans**	**11 days**	**7/1/20**	**7/16/20**	9	
12	3.1.1	**Project Work Plan**	**6 days**	**7/6/20**	**7/13/20**	4	
13	3.2	Onsite Requirements Gathering and Clarifications	3 days	7/9/20	7/13/20	9	
14	3.3	Requirements Traceability Matrix (RTM)	3 days	7/9/20	7/13/20	9	
15	3.4	**Detailed System Design (DSD) Documentation**	**52 days**	**7/13/20**	**9/22/20**	13,14	BA,SME,DHHR
16	3.4.1	**System Integration Plan (SIP)**	10 days	7/14/20	7/27/20	13,14	BA,SME,DHHR
17	3.4.2	**Import Specifications - Appendix B**	13 days	7/14/20	7/30/20	13,14	BA,SME
18	3.4.3	**WV Specifications Document**	13 days	7/14/20	7/30/20	13,14	BA,SME
19	3.4.4	**Web Services - Appendix S**	13 days	7/14/20	7/30/20	13,14	BA,SME
20	3.4.5	**Overall IVR Architecture and Flow - Appendix C**	5 days	7/14/20	7/20/20	13,14	BA,SME
21	3.4.6	**Mobile - Appendix W**	18 days	7/14/20	8/6/20	13,14	
22	3.4.7	**Compliance Reviews**	7 days	7/29/20	8/6/20	21FF	
23	4	*Task Group 1 Deliverables - Project Initiation and Project Management Task Gro*	1 day	9/23/20	9/23/20	15	PM,DHHR
24	5	**Config/Deployment**	**108 days**	**8/3/20**	**12/30/20**		
25	5.1	**Iteration 1 Config and Dev (C1)**	**30 days**	**8/3/20**	**9/11/20**		
26	5.1.1	**Configuration and Design Documentation**	**2 days**	**8/3/20**	**8/4/20**		
27	5.1.1.1	Milestone #1 - System Integration Plan Design Acceptance	2 days	8/3/20	8/4/20	16	DHHR,FD
28	5.1.1.2	Milestone #2 - Publish Test Cases & Scripts	2 days	8/3/20	8/4/20	27FF	DHHR,FD
29	5.1.1.3	Milestone #3 - Configuration and Design Document Acceptance	2 days	8/3/20	8/4/20	28FF	DHHR
30	5.1.2	**Development**	**20 days**	**8/5/20**	**9/1/20**		
31	5.1.2.1	Milestone #4 - Set Up Environments	2 days	8/5/20	8/6/20	29	FD
32	5.1.2.2	Milestone #5 - Set Up and Configure IVR	2 days	8/5/20	8/6/20		FD
33	5.1.2.3	Milestone #6 - Development Complete (Unit)	20 days	8/5/20	9/1/20		
34	5.1.3	**Testing (Team Testing)**	**8 days**	**9/2/20**	**9/11/20**		
35	5.1.3.1	Milestone #7 - Product Testing Complete (QA and CAT)	3 days	9/2/20	9/4/20	33	FD
36	5.1.3.2	Milestone #8 - User Acceptance Testing Complete	6 days	9/4/20	9/11/20	35FF	DHHR
37	5.1.4	Contract Milestone (C1)	1 day	9/11/20	9/11/20	34FF	DHHR,PM
38	5.1.5	*Task Group 2 Deliverables - Solution Planning*	1 day	9/11/20	9/11/20	37FF	PM,DHHR
39	5.2	**Iteration 2 Config and Dev (C2)**	**36 days**	**9/11/20**	**10/30/20**		
40	5.2.1	**Configuration and Design Documentation**	**2 days**	**9/11/20**	**9/14/20**		
41	5.2.1.1	Milestone #1 - Update System Integration Plan	2 days	9/11/20	9/14/20		DHHR,FD
42	5.2.1.2	Milestone #2 - Update Test Cases & Scripts	2 days	9/11/20	9/14/20	41FF	DHHR,FD

AuthentiCare West Virginia Department of Health and Human Resources (DHHR) - EVV Project Schedule (Draft)

ID	Outline Number	Task Name	Duration	Start	Finish	Predecessors	Resource Names
43	5.2.1.3	Milestone #3: Configuration and Design Document Acceptance	2 days	9/11/20	9/14/20	42FF	DHHR
44	**5.2.2**	**Development**	**25 days**	**9/11/20**	**10/15/20**		
45	5.2.2.1	Milestone #4 - Update Environments	2 days	9/11/20	9/14/20		
46	5.2.2.2	Milestone #5 - Update IVR	2 days	9/11/20	9/14/20		
47	5.2.2.3	Milestone #6 - Development Complete (Unit)	25 days	9/11/20	10/15/20		
48	**5.2.3**	**Testing (Team Testing)**	**11 days**	**10/15/20**	**10/29/20**		
49	5.2.3.1	Milestone #7 - Product Testing Complete (QA and CAT)	5 days	10/16/20	10/22/20	47	FD
50	5.2.3.2	Milestone #8 - User Acceptance Testing Complete	6 days	10/23/20	10/30/20	49	DHHR
51	5.2.4	Contract Milestone (C2)	1 day	10/30/20	10/30/20	48FF	DHHR,PM
52	**6**	**Scaled WV AuthentiCare Model Go-Live**	**43 days**	**11/2/20**	**12/30/20**		**Dev team,PM**
53	6.1	Select and Onboard Providers of different sizes	5 days	11/3/20	11/9/20	50	DHHR,FD
54	**7**	**Iteration 3 Config and Dev (C3)**	**43 days**	**11/2/20**	**12/30/20**		
55	**7.1**	**Configuration and Design Documentation**	**2 days**	**11/2/20**	**11/3/20**		
56	7.1.1	Milestone #1 - Update System Integration Plan	2 days	11/2/20	11/3/20		
57	7.1.2	Milestone #2 - Update Test Cases & Scripts	2 days	11/2/20	11/3/20	56FF	
58	7.1.3	Milestone #3 - Configuration and Design Document Acceptance	2 days	11/2/20	11/3/20	57FF	
59	**7.2**	**Development**	**30 days**	**11/3/20**	**12/14/20**		
60	7.2.1	Milestone #4 - Update Environments	2 days	11/3/20	11/4/20		
61	7.2.2	Milestone #5 - Update IVR	2 days	11/3/20	11/4/20		
62	7.2.3	Milestone #6 - Development Complete (Unit)	30 days	11/3/20	12/14/20		
63	**7.3**	**Testing (Team Testing)**	**13 days**	**12/14/20**	**12/30/20**		
64	7.3.1	Milestone #7 - Product Testing Complete (QA and CAT)	6 days	12/14/20	12/21/20		
65	7.3.2	Milestone #8 - User Acceptance Testing Complete	6 days	12/21/20	12/28/20	64FF	
66	7.4	ADA Validation Provided from Vendor	1 day	12/29/20	12/29/20	65	FD
67	7.5	Contract Milestone (C3)	1 day	12/30/20	12/30/20	63FF	DHHR,PM
68	**8**	**ORR Preparation**	**43 days**	**11/2/20**	**12/30/20**		
69	8.1	Validate scripts for evidence	5 days	11/16/20	11/20/20	44	FD CMS SME
70	8.2	Schedule 3rd party audit functions and reports	5 days	11/2/20	11/6/20	39	FD CMS SME
71	8.3	Criteria Evidence 1 - 10 generate and reviews	10 days	11/16/20	11/27/20	48SF+10 days	FD CMS SME
72	8.4	Criteria Security 1 Auditor Summary Report	2 days	12/3/20	12/4/20	71SF+15 days	FD CMS SME
73	8.5	Submit Evidence for scheduled ORR	1 day	12/4/20	12/4/20	72FF	FD CMS SME
74	8.6	Conduct Operational Readiness Review (ORR) with DHHR and CMS (TBD)	1 day	12/21/20	12/21/20	73	DHHR,FD CMS SI
75	**9**	**Operational/Helpdesk Activities**	**8 days**	**12/21/20**	**12/30/20**		
76	9.1	Phone number Helpdesk Set Up	1 day	12/21/20	12/21/20		
77	9.2	Monthly Reporting	8 days	12/21/20	12/30/20		
78	9.3	Training of Helpdesk Staff	1 day	12/22/20	12/22/20		Training Lead
79	**10**	**Training and Outreach Activities**	**193 days**	**7/1/20**	**3/29/21**		**Training Lead**
80	10.1	Training and Outreach Plan	57 days	7/1/20	9/18/20		Training Lead
81	10.2	Training	82 days	12/8/20	3/31/21		Training Lead
82	11	*Task Group 3 Deliverables - Solution Design, Testing, and Operational Readines*	1 day	2/26/21	2/26/21		DHHR,PM
83	**12**	**AuthentiCare Go/No Go Decision**	**9 days**	**12/21/20**	**12/31/20**		
84	12.1	Perform AuthentiCare Go/No Go Assessment After ORR	9 days	12/21/20	12/31/20		DHHR,FD
85	**13**	**Operations & Maintenance (Production Readiness)**	**60 days**	**1/4/21**	**3/26/21**		

AuthentiCare West Virginia Department of Health and Human Resources (DHHR) - EVV Project Schedule (Draft)

ID	Outline Number	Task Name	Duration	Start	Finish	Predecessors	Resource Names
86	13.1	Post Go Live Production Data Validation/Testing	5 days	1/4/21	1/8/21		
87	13.2	MILESTONE: Go Live Begins	0 days	1/4/21	1/4/21		
88	13.3	*Production Roll Out*	*65 days*	*1/4/21*	*4/2/21*	*87*	
89	**13.4**	**Cutover - Go-Live**	**1 day**	**1/4/21**	**1/4/21**	**88**	
90	**13.5**	**Go-Live Support**	**20 days**	**1/4/21**	**1/29/21**		
91	14	*Task Group 4 Deliverables - Solution Deployment*	1 day	1/4/21	1/4/21	89FF	DHHR,PM
92	**15**	**Closeout**	**60 days**	**1/4/21**	**3/26/21**		
93	15.1	Provide Transition Documention	10 days	1/4/21	1/15/21		FD
94	**15.2**	**Closeout Implementation and Transition to M&O Plan**	**6 days**	**1/4/21**	**1/11/21**		
95	15.3	Conduct a Transition to M&O Meeting	1 day	1/18/21	1/18/21	93	FD,DHHR
96	15.4	Conduct Implementation Project Close Out Meeting	1 day	1/19/21	1/19/21	95	FD,DHHR
97	15.5	**Implementation Project Closeout and Lessons Learned Report**	7 days	1/20/21	1/28/21	96	
98	16	*Task Group 5 Deliverables - Project Monitor and Control*	1 day	1/29/21	1/29/21		DHHR,PM
99	**17**	**Post-Implementation CMS Certification Support (Schedule TBD)**	**128 days**	**1/4/21**	**6/30/21**		
100	17.1	Provide Evidence for Post Go Live CMS Certification Requirements (TBD)	65 days	4/1/21	6/30/21	87	FD CMS SME
101	17.2	Continued Support through Stabilization Period (Duration - TBD)	128 days	1/4/21	6/30/21		FD CMS SME
102	17.3	MILESTONE: CMS Final Milestone Review Certification (TBD)	0 days	6/30/21	6/30/21	101	FD CMS SME,WD

5.0 Attachment 6: Mandatory Requirements

RFP Section 5.4.2.10 (Table 11) & Attachment 6, pp. 74 & 116

1.1 The Vendor must meet the mandatory requirements as a part of the submitted proposal. Failure on the part of the Vendor to meet any of the mandatory requirements will result in its proposal's disqualification, at the sole discretion of the Department of Health and Human Resources (DHHR). The terms "must", "shall", or "will" stipulates and identifies a mandatory requirement.

1.2 The Vendor must demonstrate compliance with mandatory requirements in its proposal. If the Vendor's proposal meets the mandatory requirements, the Vendor's Proposal may be included in the next part of the technical evaluation of this request for proposal (RFP).

1.3 For mandatory requirements that involve documentation, Vendors should include the documentation with their technical proposal. If the documentation is not provided in the technical proposal, Vendors must provide a written commitment in their proposal to provide the documentation prior to contract execution. When appropriate, Vendors must provide narrative responses in the area below.

1.3.1 See the attached Microsoft Excel® file titled, Attachment 6: Mandatory Requirements.

With the AuthentiCare solution for Electronic Visit Verification, we propose implementing and operating an innovative, low-risk, flexible, and economical EVV program that offers the best value for the West Virginia Department of Health and Human Resources (DHHR) and its stakeholders.

FDGS has examined RFP Attachment 6: Mandatory Requirements. This section provides a description of how AuthentiCare meets or exceeds every mandatory requirement. We have included a summary response for each and, where appropriate, the reference(s) to other proposal sections of our response that further detail how AuthentiCare meets or exceeds each requirement. Following the narrative response to each mandatory requirement in Table 5.1, we have included a completed Attachment 6 as required.

While we provide individual responses to each mandatory requirement, together, all of the components of the AuthentiCare EVV solution, along with the FDGS experience and supporting services, provide DHHR an end-to-end EVV solution to best support your stakeholders including state staff, providers, workers, and beneficiaries receiving services through the EVV program.

Table 5.1 – AuthentiCare meets or exceeds every mandatory requirement

Req. ID #	Requirement Text	Requirement Type
MR001	All provided services must comply with the Department rules.	Program Management
The AuthentiCare EVV solution is a configurable framework. Through a series of iterative and collaborative design and configuration sessions with DHHR, AuthentiCare is able to comply with all department rules, state and federal statutes, regulations, and rules applicable to the services described in the RFP. As EVV program policies and procedures are updated in the future, AuthentiCare provides the flexibility to update rules and workflows to quickly accommodate the latest program modifications and compliance.		
MR002	The Vendor must agree to adhere to the performance measures and penalties outlined within the service level agreements (SLAs) included in the request for proposal (RFP).	Project Management
FDGS has reviewed the service level agreements (SLAs) included in this RFP Appendix 3: Service Level Agreements and Performance Standards. FDGS agrees to adhere to performance measures and penalties within the included service level agreements. If the State awards the EVV Project to FDGS, we request the ability to enter into good faith negotiations with the State to incorporate mutually acceptable Service Level Agreements that are applicable to the SaaS-based hosted solution (AuthentiCare) and also address associated liquidated damages for any failure to meet such Service Level Agreements that are reasonably aligned with the overall project implementation and hosted solution costs to the State.		

Req. ID #	Requirement Text	Requirement Type
MR003	The Vendor must ensure that solution modules and applications integrate successfully and effectively with minimal or no customization.	Hardware and Infrastructure

AuthentiCare supports application integration and real-time interfaces through the latest industry standard specification (JSON/REST) web service transactions or, as an alternative, the standard XML file Application Programmer Interface (APIs). FDGS has extensive experience integrating with MMIS (and other statewide and MCO systems). AuthentiCare has successfully managed file API integrations with DXC MMIS in full production in Kansas, Oklahoma, and Alabama, and currently completing our pilot in Nevada.

This interface is bi-directional, accepting client and provider eligibility information as well as authorizations derived from the plan of care. As an export from AuthentiCare, 837 claim submissions historically have a high rate of successful payment—99.4 percent of first pass claims submitted from AuthentiCare to their system paid successfully, resulting in less post-adjudication adjustments and rework—because eligibility, authorization, and other items are validated on the front end, prior to 837 submission, which means that only "clean" claims are ultimately submitted for adjudication.

As a major integration point, FDGS teams have successfully worked alongside system integrators and DXC Technology in several of our AuthentiCare EVV projects. In fact, for the Nevada implementation, coordination with DXC for interfaces was essential to receiving provider and member data, and our staff was able to work with all MCOs to successfully facilitate authorizations and 837/835 integration.

Successful Record of Integration to MMIS (DXC systems)

FDGS has worked with our customers' vendors to successfully build and maintain interfaces to DXC-managed systems, and other state MMIS systems. We have a successful record of submitting claims at a high rate of accuracy. We anticipate having the same type of success integrating into the West Virginia MMIS and Managed Care systems for provider claims submissions.

99.4 percent of first-pass claims submitted from AuthentiCare to state systems paid successfully. FDGS can offer West Virginia the same success.

Currently, FDGS is integrated with DXC-operated and managed MMIS systems in:

- Oklahoma (DXC/interChange): Since beginning our operation in 2009, AuthentiCare has processed 4 million claims annually for more than 300 provider locations and 26,000 beneficiaries. 99.5 percent of first-pass submitted claims were transmitted and paid via an 837 specification compliant file to the DXC MMIS portal.
- Kansas (DXC/interChange): Since 2010, AuthentiCare has processed 4 million claims annually for more than 600 provider locations and 21,000 beneficiaries. 99.3 percent of submitted claims were transmitted via an 837 specification compliant file to the DXC MMIS portal for adjudication.
- Alabama (DXC/interChange): AuthentiCare went live on October 1, 2017. Since then, it has processed over 5 million claims. AuthentiCare exchanges 837 and 835 files via secure File Gateway with the DXC-operated and managed MMIS system. 98.9 percent of first-pass claims submitted to the DXC MMIS portal were successfully paid.

MR004	**The solution must securely capture and electronically verify:**	**Visit Verification**
MR005	The identity of the member receiving services	Visit Verification
MR006	The identity of the direct care worker making the visit	Visit Verification
MR007	The identity of the provider agency	Visit Verification
MR008	The date the visit begins and ends	Visit Verification
MR009	The time the visit begins and ends	Visit Verification
MR010	The location of the visit	Visit Verification
MR011	The services being delivered	Visit Verification

Req. ID #	Requirement Text	Requirement Type
MR012	The waiver program or plan name	Visit Verification

AuthentiCare provides multiple data methods for securely capturing visit verification details including mobile, web, and IVR. All PHI data is encrypted both at rest and in transit using industry-standard tools supporting guidelines from NIST and other security standards.

The caregiver visit data that the AuthentiCare system collects fully complies with the requirements of Section 12006 provisions under the 21st Century Cures Act, while providing additional data collection for monitoring plan of care compliance. As required by 21st Century Cures Act, the data collected and verified includes:

- The individual receiving the service [MR005]
- The individual providing the service [MR006]
- The provider agency delivering the service [MR007]
- The date(s) of the service [MR008/MR009]
- The beginning and end times of the service
- The location of the service delivery [MR010]
- The type of service performed with procedure code [MR011]
- Units of service delivered

In addition, the caregiver can conveniently record other data electronically at the time and place of service, eliminating paper timesheets and other manual processes for capturing information. This data includes:

- The waiver program or plan name [MR012]
- Plan of care activities/tasks performed
- The travel time or mileage between clients
- Caregiver observations of condition changes or unmet needs for follow up

The AuthentiCare mobile EVV application can be downloaded on mobile phones and tablets from the Apple Store or Google Play. The AuthentiCare mobile application includes "Store and Forward" technology to collect visit information in locations that may not have cellular or Wi-Fi connectivity.

Caregivers install the free mobile app on their own phone or tablet and use it to check in and check out when providing care. The system uses the device's network time and GPS location to verify the start and end times of the visit and the location of service in real-time. When using Store and Forward, visit information is encrypted and stored on the device until the worker has Wi-Fi or cellular data coverage, and then the data is automatically uploaded, making this a paperless solution. In standard mode, the mobile app uploads visit data to AuthentiCare in real time.

To meet the requirements of the 21st Century Cures Act, FDGS' primary method to support visit verification and data capture is via the AuthentiCare mobile application. FDGS also offers an Interactive Voice Response (IVR) solution as a secondary or backup alternative to the mobile application.

MR013	The solution must uniquely identify each user.	Security Management

Each AuthentiCare user of the web portal and mobile app is granted specific role-based access through the use of a unique user ID. Our minimum password policies can be configured to even higher standards at DHHR's request. Password requirements include length, strength, complexity, change frequency, and history.

MR014	The solution must have the ability to receive data from approved electronic visit verification (EVV) data partners and aggregate the external data into the overall solution, through the Department's approved file format and transfer method(s).	Data Sources, Delivery, and Display

AuthentiCare's Data Aggregator can be configured to import data so that the State has a common repository of all EVV data collected, including information that identifies which system captured the data. The AuthentiCare solution provides for an EVV interface with existing third-party EVV systems that have been approved by DHHR to send data to the AuthentiCare solution for unified statewide reporting. Using our web services provides near real-time processing of data collected through AuthentiCare's Data Aggregator.

EVV-required data, like visit data from GPS and other alternative location methods, is accepted if provided by external systems. As data are aggregated into AuthentiCare, provider reports are available for verified visits by the billing provider, visits that were not verified, and others. To maintain secure access to report data, provider agencies must securely log in to access their respective Reports pages to review their reports. AuthentiCare allows reports to be downloaded in PDF, Excel, and CSV formats.

AuthentiCare supports the calculation of total daily and weekly hours worked by the attendant, and aggregates hours

Req. ID #	Requirement Text	Requirement Type
across payers, programs, providers, and recipients receiving services through the master worker function. This collects the hours as some direct care workers may support different providers. These data are compiled through multiple sources. To aggregate across providers and payers, each direct care worker must receive a unique ID when registered by the provider. The AuthentiCare solution provides the MCOs and providers different options and capabilities to move data automatically in and out of the AuthentiCare solution so that they can choose the transport method and format most compatible with their existing systems. The process can accept data through three secure channels including web service upload (real-time communications), web portal upload (for smaller providers), and SFTP file gateway upload (for larger providers or EVV service bureaus that produce large files). Import results can be posted back to the same portal for subsequent pickup.		
MR015	The solution must be accessible for individuals with physical disabilities and vision impairments and satisfy the accessibility requirements of Section 508 of the Rehabilitation Act and the Americans with Disabilities Act (ADA).	Project Management
AuthentiCare is accessible and compliant with ADA, Section 508 and WCAG 2.0 standards. AuthentiCare is able to demonstrate substantial W3C compliance, as well as the capability to use screen reading software, like JAWS® or ZoomText®. With regard to accessibility standards, FDGS has engaged Level Access to advise us as to accessibility and use with assistive technology for the AuthentiCare Web and Mobile App. Level Access has provided third-party ADA Section 508 certification of both the Web and Mobile applications. Copies of the most recent AuthentiCare VPAT reports will be provided as part of the CMS ORR evidence for criteria EVV8 prior to go live per the CMS OBC process.		
MR016	The Vendor must establish business associate agreements (BAA) or contractual agreements with the Department and any subcontractors according to Federal agency requirements that have access to data which is subject to protection by the Health Insurance Portability and Accountability Act (HIPAA). (Reference: https://www.hhs.gov/hipaa/index.html)	Security Management
FDGS agrees to enter into and sign a Business Associate Agreement (BAA) with the Department according to Federal agency requirements for access to data, which is subject to protection by the Health Insurance Portability and Accountability Act (HIPAA).		
MR017	The Vendor must agree to enter into applicable Business Associate Agreements (BAA) with external electronic visit verification (EVV) data partners as directed by the Department prior to accepting or exchanging protected health information (PHI) and/or personally identifiable information (PII) data from the EVV solution.	Security Management
FDGS agrees to enter into and sign a Business Associate Agreement (BAA) with external EVV data partners as directed by the Department prior to accepting or exchanging protected health information (PHI) and/or personally identifiable information (PII) data from the EVV solution.		
MR018	The Vendor must ensure that all data submitted to or collected by the solution will remain the property of the Department.	Security Management
FDGS agrees that all data submitted to or collected by the AuthentiCare EVV solution will remain the property of the Department.		
MR019	The Vendor must agree to abide by all the Department security and privacy policies to protect confidential and sensitive information.	Security Management
FDGS understands the necessity of protecting the privacy and confidentiality of your data. We have reviewed the Department security and privacy policies protecting confidential and sensitive information and agree to abide by all Department security and privacy policies to protect confidential and sensitive information. Our current technical and operational practices meet or exceed the Department's security and privacy policies. The AuthentiCare team will work with the Department to continue to meet related policies as they mature throughout the life of the contract. The AuthentiCare solution provides world-class security thanks to our Fiserv corporate global security practices and procedures. The AuthentiCare EVV system meets the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA-compliant practices include: • Data transfers employ AES 256-bit encryption and TLS 1.2 or SFTP • Users are individually registered and functional rights and roles are assigned to their login credentials • Both IVR and Mobile App employ two-factor authentications as required • Users are data scoped to see only relevant data for which they have permission to view • ANSI X-12 transactions are employed where relevant Security risk assessment, policies, and procedures are assessed annually by three third-party assessors for SSA-18		

Req. ID #	Requirement Text	Requirement Type
SOC1, PCI-DSS, and GLBA compliance. The CMS definition of HIPAA compliance in NIST SP 800-66 maps directly to PCI-DSS and SSA-18 audited controls.		
MR020	The solution must have the ability to receive, store, and exchange protected health information (PHI) and personally identifiable information (PII) through authentication, along with encryption methods to secure sensitive information following nationally recognized standards, including the privacy and security controls outlined within National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations special publication (SP) 800-53 (moderate) and NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices. (Reference: https://csrc.nist.gov/publications/detail/sp/800-111/final and https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)	Security Management
In the AuthentiCare EVV system solution, Medicaid data necessary to perform the duties as outlined in this RFP are stored in a secure and confidential manner that meets Health Insurance Portability and Accountability Act of 1996 (PL 104-191) (HIPAA) requirements. This includes HIPAA requirements related to privacy, security, transaction code sets, and medical provider enumeration. On an ongoing basis, our policies are reviewed and approved by these three broadly recognized assessors—SOC 1/SSAE-18 (Ernst & Young), PCI DSS (Trustwave), and GLBA (Federal Financial Institutions Examination Council [FFIEC])—as well as many state, local, and customer assessors. FDGS has established a Global Cyber Security Policy in alignment with the NIST CSF (National Institute of Standards and technology, Cyber Security Framework), which is based on a subset of controls within the comprehensive NIST SP 800-53 r4 controls. The Global Cyber Security Policy is fully complementary to the ISO (International Standards organization) 27001-2013 cyber security controls; with certain geographic areas maintaining ISO 27001-2013 certification. In support of NIST SP 800-111 guidelines, our solution processes employ security standards including TLS 1.2 Transport Level Security protocol, SFTP protocol for managed file transfers, and certificate authentication for file transfer portals. AES 256-bit encryption, together with these protocols, meets the secure standards required for exchange of protected health information (PHI) under HIPAA and HITECH.		
MR021	The solution must use only Federal Information Processing Standard (FIPS) Pub 140-2 validated (or higher) encryption or equivalent. (Reference: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf, and https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf)	Security Management
AuthentiCare uses only Federal Information Processing Standard (FIPS) Pub 140-2 validated (or higher) encryption or equivalent. For all web and web service connections to the AuthentiCare platform, FDGS requires TLS 1.2 Transport Level Security (which includes SHA 2) and RSA 2048 keys. (TLS 1.0 and 1.1 and SSLv3 connections were deemed not sufficiently secure and were discontinued in 2016.) File transfers use FDGS' hosted SFTP site, and are AES 256-bit encrypted according to FIPS 140-2 requirements.		
MR022	The Vendor must remain in alignment with all future updates to Centers for Medicare & Medicaid Services' (CMS') certification processes and any future updates to the Medicaid Enterprise Certification Toolkit (MECT) (Reference: https://www.medicaid.gov/medicaid/data-and-systems/mect/index.html)	CMS Certification
FDGS will remain in alignment with all future updates to Centers for Medicare & Medicaid Services' (CMS') certification processes and any future updates to the CMS EVV Outcomes Based Certification guidelines. With FDGS, DHHR gains the capabilities of our government consulting practice along with our healthcare industry leadership. Our government consulting practice is integrated with the AuthentiCare team to maintain its alignment with the dynamic program and policy from CMS. The flexible and configurable platform of AuthentiCare has proven to be an adaptable solution to support both the program changes from CMS and their evolving requirements. The AuthentiCare Delivery organization includes a Compliance Team of experts in CMS policy, MITA, security and privacy, HIPAA, federal standards and industry best practices. The Compliance team continuously monitors for new requirements, taking a proactive approach with timely inputs to the AuthentiCare product roadmap for continued compliance. CMS considers EVV solutions to be a Medicaid enterprise module and a candidate for certification to qualify for enhanced funding for DDI and M&O phases. FDGS knows the certification process and has developed its practices based on continually monitoring and analyzing new laws, rules, regulations, standards, and best practices. Our SMEs in Medicaid policy, MITA, cybersecurity, and CMS Medicaid Enterprise Systems, as well as our experience with multiple AuthentiCare implementations, provide key input to the AuthentiCare product roadmap and delivery practice		

Req. ID #	Requirement Text	Requirement Type

services. The AuthentiCare solution for DHHR supports expansion into additional home healthcare programs, and continued benefits of fraud prevention, quality and program integrity metrics, and continued cost savings.

Our extensive experience with MECL and MECT certification provided us the insight to ask CMS defining questions during their finalization of the newly released EVV Outcomes Based Certification (OBC release 1.0) process and guidelines. CMS considers the new OBC process to be outside the MECL process and a unique solution for EVV certification that is streamlined and with a timeframe that fits a COTS/SaaS solution. The Department will need to report quarterly four major Key Performance Indicators (KPIs), and annually on the fifth KPI with the Department's review of security and privacy risk assessment. FDGS is well positioned and experienced to advise the Department on these latest requirements and guidelines for certification of the EVV solution.

Our consulting teams have worked with CMS in all five of their newly defined regions. From coast to coast, we demonstrate our professional expertise, insight, and healthcare leadership to our clients and CMS. Because our consulting team works on other Medicaid Enterprise System projects, we have the in-depth understanding of the modular approach to modernization the EVV program, Medicaid policies, MITA, and the Standards and Conditions, bringing the broader enterprise view to EVV solutions and implementations. Our CMS and Medicaid SMEs are part of the AuthentiCare delivery resources enhancing the depth of knowledge in delivering and supporting West Virginia in the ever-evolving Medicaid and healthcare industry.

MR023	The Vendor must design the solution to support the Medicaid Information Technology Architecture (MITA) goals for the Department as defined in the Department's MITA State Self-Assessment (SS-A) and other West Virginia MITA artifacts provided in the WV EVV RFP Procurement Library.	CMS Certification

From Addendum 6 to this RFP, we understand that the Department will release its most recent MITA State Self-Assessment upon award.

FDGS has reviewed publically available information regarding the 2015-2016 MITA State Self-Assessment (SS-A) and related MITA artifacts from the procurement library and West Virginia web sites. Our EVV solution is part of the Medicaid enterprise and support MITA 3.0.

AuthentiCare's integration capabilities are based entirely on open-systems standards and accommodate communications to database management systems and back-end solutions through APIs and custom imports and exports. Additional features, like Microsoft's BizTalk EDI 837 file creation, are built into the AuthentiCare solution and leverage the open standard architecture. AuthentiCare's feature-rich solution supports MITA's seven conditions and standards, as well as the Department's goals pertaining to MITA.

Modularity Standard

AuthentiCare employs a modular, flexible approach to systems development, including the use of open interfaces and exposed application programming interfaces (APIs) to separate business rules from core programming. This also makes business rules available in formats that both humans and computers can read. Most business rules in AuthentiCare are captured in metadata tables in the database so that we can easily change and update them as business rules change. The core programs in AuthentiCare use business rules that are dynamically data-driven by values in meta-tables. This separates the core functions from a specific client's setup and business rules. This meets the modularity standards requirement to separate APIs, business rules, and core code into modules.

MITA Condition

FDGS uses the MITA conditions and standards for the development and deployment of the AuthentiCare EVV solution. We have a strong understanding of MITA and its emerging industry changes. Our knowledge of MITA and Medicaid Enterprise Systems' modular approach, architecture, and platforms will benefit DHHR in the integration of our EVV solution with your Medicaid modernization plans and increasing MITA maturity.

Industry Standards Condition

Our AuthentiCare solution architecture and design applies industry standards whenever applicable industry standards exist. This makes the solution highly modular, extensible, interoperable, and flexible.

The AuthentiCare solution incorporates multiple industry standards across its platform:

- Data transfer methods including Web Service (WS) standards and specifications: JSON-WDP, REST, UDDI, WSDL, WS-Federation, WS-Management, WS-Metadata Exchange, WS-Policy, WS-Security, WS-Reliable Messaging, and WS-Transaction
- Standard XML file Application Programmer Interface (APIs) hosted by Fiserv
- Established Global Cyber Security Policy in alignment with the NIST CSF (National Institute of Standards and

Req. ID #	Requirement Text	Requirement Type

technology, Cyber Security Framework), which is based on a subset of controls within the comprehensive NIST SP 800-53 r4 controls

- Global Cyber Security Policy is fully complementary to the ISO (International Standards organization) 27001-2013 cyber security controls; with certain geographic areas maintaining ISO 27001-2013 certification
- Certified controls from PCI-DSS and SSAE-18 map to and cover applicable HIPAA security controls as specified in NIST SP800-66 r1 Appendix D: *HIPAA Security Rule Standards and Implementation Specifications Crosswalk*
- ANSI X-12 transactions are employed where relevant

Leverage Condition

The AuthentiCare solution is inherently a Software-as-a-Service (SaaS) solution and its interfaces are sharable and reusable within West Virginia agencies. In particular, the Mobile App supports multiple configurations with different business rules. The business rules set is selected by a configuration code, while user preferences are applied when the user logs in. This is achieved with only one common app each in the Apple App Store and Google Play.

The AuthentiCare solution is in full production in several states, with each state having the solution modules relevant to their specific business and program needs.

Business Results Condition

The AuthentiCare solution is a modular, flexible, extensible, interoperable, service oriented architecture (SOA)-based system that provides near real-time EVV data. This supports accurate and timely claims processing and effective communication for all DHHR users, providers, applicants, beneficiaries, and plans. MMIS claim payment rates are typically in excess of 99 percent, so providers have few denied claims, reducing rework for both providers and Department staff. By only allowing billing for documented services delivered, states typically see a 5–12 percent spending reduction by not paying for missed or shortened visits. The best providers have a renewed focus on quality of care and providing all of the services beneficiaries are supposed to receive.

The AuthentiCare solution from FDGS has a record of cost savings for state Medicaid agencies through accurate and timely claims processing. By selecting AuthentiCare, DHHR can achieve its business objectives of cost savings, reduced fraud, and compliance with 21st Century Cures Act.

Reporting Condition

AuthentiCare comes with a robust web and reporting solution that provides information to support program evaluation, continuous improvement in business operations, transparency, and accountability. Ad hoc queries provide management with additional reporting capabilities. Additional details regarding AuthentiCare reporting capabilities are included in our responses to the detailed requirements from Appendix 1 – Detailed Specifications.

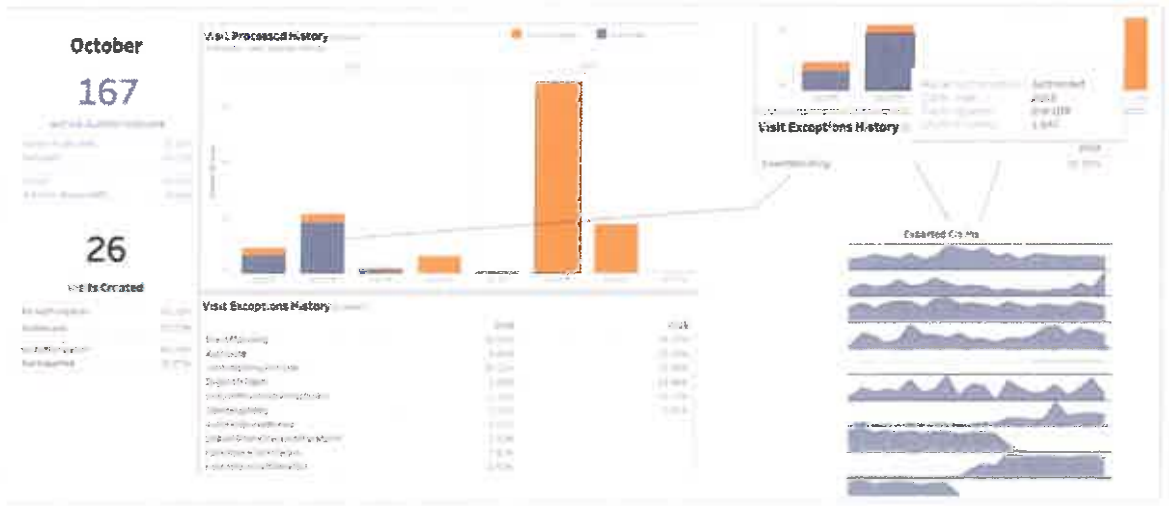


Figure 5.1 – Dashboards for both real-time and historic information

Req. ID #	Requirement Text	Requirement Type
	Interoperability Condition AuthentiCare's EVV solution architecture is based on a Service Oriented Architecture (SOA), and these services are available for other customer-approved system consumption external to EVV. FDGS adopted SOA to meet our customers' current and future business requirements while meeting security, scalability, reliability, and availability requirements. The SOA architecture will be beneficial for DHHR using the AuthentiCare integration with its MMIS platform. The AuthentiCare solution can be integrated into a larger SOA architecture using data interfaces and application programming interfaces (API) and accessed by any Medicaid enterprise application in need of our services. AuthentiCare solution processes employ data interchange and web service standards including secure JSON API and restful (REST) web services. This API infrastructure has been proven in production operations for over five years.	
MR024	The Vendor must coordinate with the Department to develop all documentation required by Centers for Medicare & Medicaid Services' (CMS') Certification process as defined in the most recent Medicaid Enterprise Certification Toolkit (MECT). (Reference: https://www.medicaid.gov/medicaid/data-and-systems/mect/index.html)	CMS Certification
	FDGS offers hands-on experience in applying our Project Management methodology to support CMS certification via the CMS EVV Outcomes Based Certification. From our work with CMS in other states, we know that CMS certification of the EVV solution is required to receive and maintain enhanced funding. Our Subject Matter Experts have been engaged with CMS and our customers through the finalization and implementation of the new EVV Outcomes-Based Certification process and related guidelines. FDGS agrees to coordinate with the Department for all required criteria evidence and audits in support of the CMS Certification process. Our Certification SME will work with the West Virginia EVV project from project initiation through the CMS Certification process approval. Our Certification SME will work with DHHR as an integral member of the AuthentiCare delivery team. At project initiation, they will review the current CMS, HIPAA, NIST, and other mandated requirements that may impact the scope, configuration, and implementation; participate in design and delivery; and prepare for the Operations Readiness Review prior to Go-Live. Post Go-Live, our Certification SME will stay engaged with the customer and CMS in the delivery of Key Performance Indicator reports and preparation for the final certification review meeting. This proactive approach to CMS EVV OBC certification supports the necessary timing of evidence delivery under OBC meeting CMS' requirements for certification. Based on the approved project scope and validated functional and system requirements, including those necessary for CMS Certification, FDGS will correct problems or defects preventing CMS Certification at no additional cost to DHHR. Additional details regarding CMS Certification and how FDGS integrates the certification activities into our overall approach to the AuthentiCare SDLC are included in Proposal Section 8.5 CMS Certification.	

5.1 Completed Attachment 6: Mandatory Requirements

FDGS provides the completed Excel version of Attachment 6: Mandatory Requirements on the following pages.

Mandatory Requirements							
Req ID #	RTM ID	Hierarchy Level	Requirement Text	Type	Attachment	Section	Page #
MR001	5207	1	All provided services must comply with the Department rules.	Program Management	Attachment 6 - Mandatory Requirements	Section 5.0 Section 6.2	5-1 6-17
MR002	5296	1	The Vendor must agree to adhere to the performance measures and penalties outlined within the service level agreements (SLAs) included in the request for proposal (RFP).	Project Management	Attachment 6 - Mandatory Requirements	Section 5.0 Section 8.1	5-1 8-10
MR003	4762	1	The Vendor must ensure that solution modules and applications integrate successfully and effectively with minimal or no customization.	Hardware and Infrastructure	Attachment 6 - Mandatory Requirements	Section 5.0 Section 7.3	5-2 7-28
MR004	4333	1	The solution must securely capture and electronically verify:	Visit Verification	Attachment 6 - Mandatory Requirements	Section 5.0 Section 6.1	5-3 6-4
MR005	4334	2	The identity of the member receiving services	Visit Verification	Attachment 6 - Mandatory Requirements	Section 5.0 Section 6.1	5-3 6-4
MR006	4339	2	The identity of the direct care worker making the visit	Visit Verification	Attachment 6 - Mandatory Requirements	Section 5.0 Section 6.1	5-3 6-4
MR007	4181	2	The identity of the provider agency	Visit Verification	Attachment 6 - Mandatory Requirements	Section 5.0 Section 6.1	5-3 6-4
MR008	4335	2	The date the visit begins and ends	Visit Verification	Attachment 6 - Mandatory Requirements	Section 5.0 Section 6.1	5-3 6-4
MR009	4336	2	The time the visit begins and ends	Visit Verification	Attachment 6 - Mandatory Requirements	Section 5.0 Section 6.1	5-3 6-4
MR010	4337	2	The location of the visit	Visit Verification	Attachment 6 - Mandatory Requirements	Section 5.0 Section 6.1	5-3 6-4
MR011	4338	2	The services being delivered	Visit Verification	Attachment 6 - Mandatory Requirements	Section 5.0 Section 6.1	5-3 6-4
MR012	5180	2	The waiver program or plan name	Visit Verification	Attachment 6 - Mandatory Requirements	Section 5.0 Section 6.1	5-3 6-4
MR013	4341	1	The solution must uniquely identify each user.	Security Management	Attachment 6 - Mandatory Requirements	Section 5.0 Section 7.4	5-3 7-40
MR014	3984	1	The solution must have the ability to receive data from approved electronic visit verification (EVV) data partners and aggregate the external data into the overall solution, through the Department's approved file format and transfer method(s).	Data Sources, Delivery, and Display	Attachment 6 - Mandatory Requirements	Section 5.0 Section 7.1	5-3 7-4

Mandatory Requirements							
Req ID #	RTM ID	Hierarchy Level	Requirement Text	Type	Attachment	Section	Page #
MR015	4342	1	The solution must be accessible for individuals with physical disabilities and vision impairments and satisfy the accessibility requirements of Section 508 of the Rehabilitation Act and the Americans with Disabilities Act (ADA).	Project Management	Attachment 6 - Mandatory Requirements	Section 5.0 Section 8.1	5-4 8-10
MR016	4221	1	The Vendor must establish business associate agreements (BAA) or contractual agreements with the Department and any subcontractors according to Federal agency requirements that have access to data which is subject to protection by the Health Insurance Portability and Accountability Act (HIPAA). (Reference: https://www.hhs.gov/hipaa/index.html)	Security Management	Attachment 6 - Mandatory Requirements	Section 5.0 Section 7.4	5-4 7-40
MR017	4343	1	The Vendor must agree to enter into applicable Business Associate Agreements (BAA) with external electronic visit verification (EVV) data partners as directed by the Department prior to accepting or exchanging protected health information (PHI) and/or personally identifiable information (PII) data from the EVV solution.	Security Management	Attachment 6 - Mandatory Requirements	Section 5.0 Section 7.4	5-4 7-40
MR018	4340	1	The Vendor must ensure that all data submitted to or collected by the solution will remain the property of the Department.	Security Management	Attachment 6 - Mandatory Requirements	Section 5.0 Section 7.4	5-4 7-40
MR019	5216	1	The Vendor must agree to abide by all the Department security and privacy policies to protect confidential and sensitive information.	Security Management	Attachment 6 - Mandatory Requirements	Section 5.0 Section 7.4	5-4 7-40
MR020	4841	1	The solution must have the ability to receive, store, and exchange protected health information (PHI) and personally identifiable information (PII) through authentication, along with encryption methods to secure sensitive information following nationally recognized standards, including the privacy and security controls outlined within National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations special publication (SP) 800-53 (moderate) and NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices. (Reference: https://csrc.nist.gov/publications/detail/sp/800-111/final and https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)	Security Management	Attachment 6 - Mandatory Requirements	Section 5.0 Section 7.4	5-5 7-40
MR021	5155	1	The solution must use only Federal Information Processing Standard (FIPS) Pub 140-2 validated (or higher) encryption or equivalent. (Reference: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf, and https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf)	Security Management	Attachment 6 - Mandatory Requirements	Section 5.0 Section 7.4	5-5 7-40

Mandatory Requirements							
Req ID #	RTM ID	Hierarchy Level	Requirement Text	Type	Attachment	Section	Page #
MR022	4346	1	The Vendor must remain in alignment with all future updates to Centers for Medicare & Medicaid Services' (CMS') certification processes and any future updates to the Medicaid Enterprise Certification Toolkit (MECT). (Reference: https://www.medicaid.gov/medicaid/data-and-systems/mect/index.html)	CMS Certification	Attachment 6 - Mandatory Requirements	Section 5.0 Section 8.5	5-5 8-48
MR023	4344	1	The Vendor must design the solution to support the Medicaid Information Technology Architecture (MITA) goals for the Department as defined in the Department's MITA State Self-Assessment (SS-A) and other West Virginia MITA artifacts provided in the WV EVV RFP Procurement Library.	CMS Certification	Attachment 6 - Mandatory Requirements	Section 5.0 Section 8.5	5-6 8-48
MR024	4345	1	The Vendor must coordinate with the Department to develop all documentation required by Centers for Medicare & Medicaid Services' (CMS') Certification process as defined in the most recent Medicaid Enterprise Certification Toolkit (MECT). (Reference: https://www.medicaid.gov/medicaid/data-and-systems/mect/index.html)	CMS Certification	Attachment 6 - Mandatory Requirements	Section 5.0 Section 8.5	5-8 8-48

6.0 Attachment 7: Business Specifications Approach

RFP Section 5.4.2.10 (Table 11), Attachment 7, & 4.4.1, pp. 74, 115, 50
1.1 The Vendor should provide a narrative overview of how the proposed system will meet the business specifications. Use the response sections to provide specific details of the proposed approach to meeting the business specifications in each subject matter area.
1.2 Responses should reference specifications and relevant mandatory requirements using the appropriate IDs from Appendix 1: Detailed Specifications and Attachment 6: Mandatory Requirements.
1.3 DHHR also expects the Vendor to propose its approach for meeting any specifications included in RFP Section 4: Project Specifications.
1.4 Responses in this section should be highly focused on the business processes and specifications and not simply provide generic or marketing descriptions of solution capabilities.
1.5 If the Vendor is proposing a phased implementation, the Vendor should indicate how that approach may or may not affect functionality. Additionally, the Vendor should indicate exception handling processes where appropriate and any dependencies on existing systems or components of the new system to provide the specified functionality.

With AuthentiCare, we can best meet your business specifications with our innovative, low-risk, flexible, and economical EVV program offering the best value for the West Virginia Department of Health and Human Resources (DHHR) and its stakeholders.

In this and the following sections, FDGS describes how AuthentiCare meets your detailed requirements from RFP Appendix 1: Detailed Specifications and the respective requirements from Attachment 6: Mandatory Requirements. Following an introduction to each Subject Matter Area from Appendix 1 (as laid out in RFP Table 11 Expected Proposal Sections and Content Structure), we provide a descriptive response to show DHHR how AuthentiCare will meet each detailed requirement.

Our subject matter experts have examined the RFP to develop our solution and assess the requirements included in this RFP. They were directed to determine the best approach for DHHR and its needs for the EVV solution. With an aggressive implementation period of only six months and the 21st Century Cures Act deadline of January 1, 2021, we determined that a focused approach to Go Live is necessary. Our approach systematically focuses on the business and technical specification provided in this RFP, Appendix 1.

We have provided Appendix 1 as required by the RFP, but plan to work with the Department to diligently identify those requirements, features, and functions of the AuthentiCare EVV implementation to:

3. Verify and validate all EVV capabilities are included to fully comply with the 21st Century Cures Act
4. Include all requirements and capabilities needed to certify West Virginia's EVV solution CMS according to their Outcomes Based Certification guidelines and processes

With this focused approach to the initial implementation period, FDGS will work with the Department to validate all requirements necessary for Go Live according to the priority business and technical specifications, iteratively complete the design and configuration specific to West Virginia's program policy, and deploy a fully functional EVV solution to meet Cures Act compliance and prepare the Department for the CMS certification steps.

Upon award, FDGS will lay out an initial plan for proposed future releases to include the additional features and functions necessary to support the remaining requirements noted as "Will Meet" in Appendix 1 – Detailed Specifications.

FDGS recognizes that West Virginia is seeking an EVV system that will meet the requirements of the 21st Century Cures Act, including the specialized requirements of DHHR and its stakeholders. The model we propose is currently operational in 11 statewide implementations, similar in size and scope to West Virginia's needs. This section explains why our approach is in West Virginia's best interest.

We are responding with our proven solution based on a fully hosted model. Our hosted approach brings a number of benefits to DHHR and its constituents:

- Provides superior security controls
- Scales cost-effectively by balancing infrastructure costs across the volumes of many clients
- Offers flexible and responsive updates to all our clients as Medicaid rules change, thus maintaining compliance with policy updates or program changes
- Keeps our solution up to date for all clients as new technologies and functions are made available
- Provides a cost-effective solution for the West Virginia

AuthentiCare can support DHHR in its mission to promote and provide appropriate health and human services for the people of West Virginia to improve their quality of life. Our AuthentiCare EVV solution assists eligible individuals with remaining in their own homes by preventing premature placement in long-term care facilities.



FDGS is committed to verifying that DHHR is compliant with the regulations of the 21st Century Cures Act with the AuthentiCare EVV Solution. AuthentiCare is a complete EVV solution that electronically verifies aspects of personal care and home health services. AuthentiCare helps you to offer your providers or MCOs a minimally burdensome, HIPAA-compliant system based on existing best practices. This section describes how selecting AuthentiCare as your EVV solution supports the State's goal of compliance with the 21st Century Cures Act.

FDGS understands that the EVV solution must also follow federal and state standards for implementation and operations, meet its functional and technical requirements, and provide a high-quality, secure environment to support an ongoing business model every day of the year.

FDGS has examined every aspect of this RFP and has provided responses to address each requirement in the Appendix 1: Detailed Specifications. We provide individual responses to each requirement, but together, all of these components of the AuthentiCare EVV solution, along with

the FDGS experience and supporting services, provide DHHR an end-to-end EVV solution to best support your stakeholders including state staff, providers, workers, and beneficiaries receiving services through the EVV program.

In this section, FDGS provides a focused response to address the subject matter areas requested within Attachment 7 – Business Specifications Approach:

- Visit Verification
- Program Management
- Program Integrity

6.1 Visit Verification

RFP Section Attachment 7 – 2-2.1 & 4.4.1.1, pp. 117, 51
2. Visit Verification
2.1 Refer to the relevant business specifications located in Appendix 1: Detailed Specifications and pertinent narrative in Section 4: Project Specifications in this RFP to cover solution capabilities in this area. The Vendor should describe its approach to Visit Verification below. The narrative response for this category should be organized using the appropriate subject matter area as per Appendix 1: Detailed Specifications.

This sub-section describes our approach to Visit Verification. Our AuthentiCare solution for EVV has been developed to support both federal and state program policy. AuthentiCare provides DHHR a complete EVV solution including the automated verification of visits using a combination of methods including mobile, web, and IVR. FDGS provides additional detail in this sub-section to meet the mandatory requirements listed in Table 6.1 as part of RFP Attachment 6 – Mandatory Requirements.

Table 6.1 – AuthentiCare Meets all Mandatory Requirements for Visit Verification

Met	Req ID #	Requirement Text
☑	**MR004**	The solution must securely capture and electronically verify:
☑	**MR005**	The identity of the member receiving services
☑	**MR006**	The identity of the direct care worker making the visit
☑	**MR007**	The identity of the provider agency
☑	**MR008**	The date the visit begins and ends
☑	**MR009**	The time the visit begins and ends
☑	**MR010**	The location of the visit
☑	**MR011**	The services being delivered
☑	**MR012**	The waiver program or plan name

AuthentiCare offers all necessary features and functions to support the DHHR EVV programs. In addition to the required data collection of the 21st Century Cures Act information, AuthentiCare provides the following major functional areas:

- Automated and manual visit verification supported by mobile, web, and IVR options
- Automated and manual scheduling of authorized services
- Alert generation for upcoming and missed visits
- Automated claims processing with configurable exception process
- Pre-defined and ad hoc reporting capabilities built into the user interface

Cultivating Convenience: AuthentiCare Mobile

- In 2019, providers submitted **10 percent more claims** via the AuthentiCare Mobile App than in 2018.
- AuthentiCare processed more than **6 million claims** via the AuthentiCare Mobile App in 2019.
- The **free** AuthentiCare mobile app is available on **Google Play** and the **Apple App Store**.

FDGS realizes that many recipients live in rural areas with little or no cellular connectivity or

internet connections. AuthentiCare offers a complete mobile application with Store and Forward technology to collect visit information in locations that may not have cellular connectivity. In addition, FDGS offers IVR as an alternative for verifying visits when a mobile device is not available. This flexibility gives users options that other solutions may not. Finally, when neither of these methods is available, we offer a fixed-location visit verification card as an optional alternative.

AuthentiCare offers multiple technology options for the data collection necessary to verify visit information. Our hosted solution includes mobile app (iOS and Android) and IVR (landline telephone, VOIP phone, or cell phone) to fully cover all statewide EVV activities. The business processes in AuthentiCare verify the time in and out, location, task performance activities, individual delivering services, and individual receiving services. Our various technology options provide an automatic backup option if there are connectivity issues at the recipient's location. These options also give service providers and clients choices based on their preferences and needs.

No matter how caregivers check in and out of AuthentiCare, it verifies each of the data elements required by the 21st Century Cures Act for each service. Table 6.2 describes how AuthentiCare validates visit data using the mobile app and IVR.

Table 6.2 – Verification Methods for AuthentiCare Mobile App and IVR

Electronically Verified Data	Mobile App	IVR
The type of service performed	The worker checks in for a service scheduled by the provider. Or the worker selects service type from a list of services authorized for the recipient.	When workers check in for a visit, they are required to identify the service that they will be providing from a menu of relevant options.
The individual receiving the service	The worker checks in for a scheduled visit by the provider, or the App identifies the GPS coordinates and presents the recipient's name to the worker to confirm based on those coordinates. If no individual is identified based on the GPS location, the worker has the option to identify by entry of a recipient ID.	The IVR presents the recipient's name to the worker to confirm based on the registered phone number. If no individual is identified based on the registered phone, the worker has the option to identify by entry of a recipient ID.
The date of service	The App records the date based on the device's clock settings. If manual time settings are enabled, the App will not allow the worker to check-in or out.	The data center's date is used as the date for the claim or encounter.
The location of service delivery	The worker's device records GPS coordinates at check-in and check-out only and matches them to the geo-fence surrounding the recipient's home or location of care. The App does not allow users to check in or out if they use mock coordinates.	The recipient's landline phone is linked to their location. When the worker calls from the landline, AuthentiCare compares the ANI to registered coordinates for the recipient to validate that the worker is in the correct delivery location.
The individual providing the service	Workers register their devices and log in using their unique user ID and password. The AuthentiCare system authenticates the user's credentials to verify that the registered direct care worker is authorized to deliver services to that recipient.	The worker provides an ID at the beginning of each check-in or check-out call. AuthentiCare compares the worker ID to the information in the system to validate that the worker is authorized to provide services to the recipient.
The time the service begins and ends	The App records the exact time, based on the device's clock settings, when the worker checks in and out. The App does not allow the worker to check-in or out if it	The system uses the system time that it receives calls at the beginning and end of the service.

Electronically Verified Data	Mobile App	IVR
	detects the use of manual time settings.	

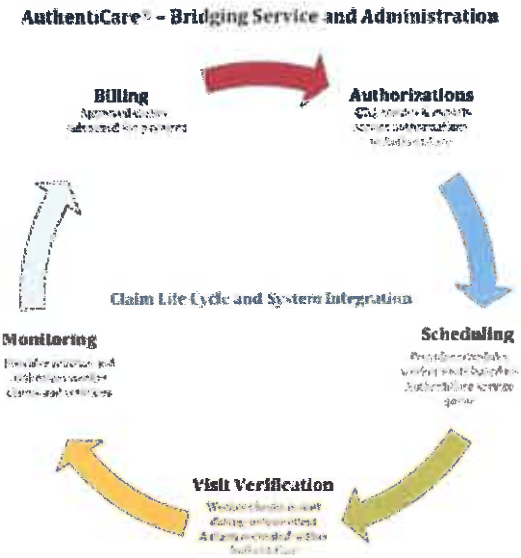
AuthentiCare meets all requirements of section 12006 of the 21st Century Cures Act. Our flexible solution is built to gather all of the visit verification data necessary for EVV programs today. The configurable solution allows us to quickly prepare AuthentiCare to support the DHHR EVV program policies and procedures.

Table 6.3 – Detailed Response to Visit Verification Requirements

Req. ID #	Requirement Text	Requirement Type
VV001	The solution should have the ability to verify the delivery of electronic visit verification (EVV) services for multiple programs with different rules and edits.	Visit Verification
AuthentiCare provides a flexible and configurable solution for verifying the delivery of EVV services of multiple programs that require unique rules and edits. Through a series of iterative design sessions, we configure AuthentiCare to support the unique rules and edits by program and by service type, if appropriate.		
VV002	The solution should have the ability to make a complete set of visit-related data elements submitted for verification available for monthly reporting and as requested by the Department, including, but not limited to:	Visit Verification
VV003	Individual receiving services	Visit Verification
VV004	Direct care worker	Visit Verification
VV005	Billing provider agency	Visit Verification
VV006	Location of visit	Visit Verification
VV007	Date of visit	Visit Verification
VV008	Visit start time	Visit Verification
VV009	Visit finish time	Visit Verification
VV010	Missed visits	Visit Verification
VV011	Late visits	Visit Verification
VV012	Services delivered, including billing code and modifiers	Visit Verification
VV013	Independent verification by individual receiving services	Visit Verification
VV014	Payer	Visit Verification
VV015	Manual or electronic verification	Visit Verification
VV016	Data collection system, including the Department solution and other approved third party electronic visit verification (EVV) systems	Visit Verification
Along with the minimum set of data elements required by the 21st Century Cures Act, as described in Table 6.2 above, AuthentiCare captures each of the data elements in requirements VV003 – VV016. The configurable framework of our AuthentiCare solution for EVV allows us to offer DHHR a flexible solution that is easily updated as federal and state EVV program policy changes.		
VV017	The solution should have the ability to integrate the scheduling, authorization monitoring, visit verification, and billing.	Visit Verification

Req. ID #	Requirement Text	Requirement Type

AuthentiCare integrates all of the components of the EVV program including scheduling, authorization monitoring, visit verification, and billing. By bringing all of the data and business processes under a single solution, DHHR can realize additional capabilities including reporting and analysis of program details over time.



The AuthentiCare mobile app and IVR are integrated with an AuthentiCare solution, web portal, web service, file management, EDI (for example, 837 claim submission), and reporting subsystems to provide full lifecycle management of recipient care from authorization, to scheduling, to visit verification and monitoring, and to billing. All visit data is evaluated against the prior authorization during the claims edit process to so that only authorized visits are submitted for payment.

The EVV process begins with data imports typically from MMIS that includes recipient information, authorizations, provider data, caregiver data, and plans of care. The AuthentiCare solution uses this to enable providers to easily schedule visits. The solution captures the visit information in real time whether coming in through the IVR or mobile application. The visit information is then available for reporting and once confirmed by the provider can be exported for billing. This supports clear planning and oversight for service delivery, and quick billing and payment for providers.

AuthentiCare monitors authorization utilization by claims. When a claim is entered, the actual and authorized units are automatically calculated and displayed to the provider on the Claim Acknowledgment Page as shown below:

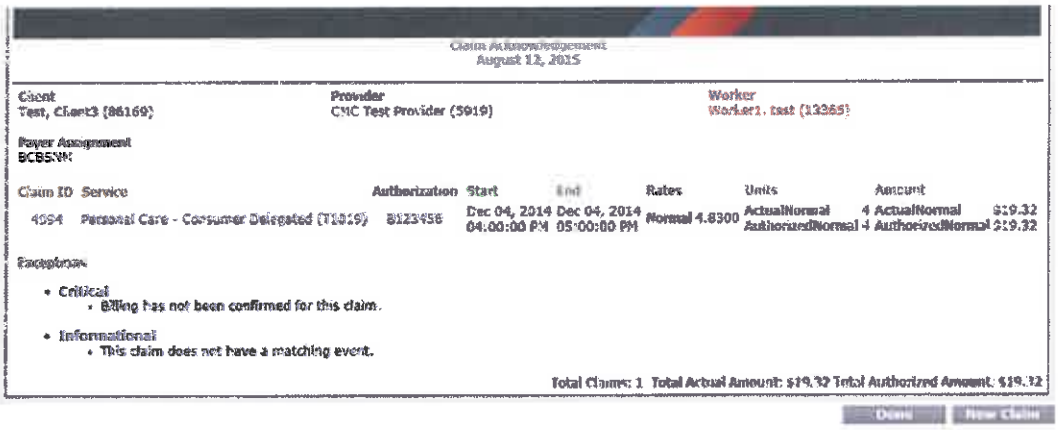


Figure 6.1 – AuthentiCare Claim Acknowledgement Page

If no authorization units remain, the claim receives a critical exception and cannot be billed. Instead the claim is included in the Exception Dashboard for the provider to review and, possibly, take corrective action.

Authorizations Received Post Service

Many states have had issues with delayed authorizations causing claims to have critical exceptions, particularly for newly enrolled recipients. AuthentiCare has a nightly background process that reviews visits for cases where a new or updated authorization received that day would potentially change the exception status of a past unbilled claim. These are then automatically reprocessed through the visit workflow so that the new authorization units are automatically applied and the status is updated. This automated process saves providers from administrative work when authorizations arrive after services have been rendered, and it provides a means of delaying the billing of claims that would be rejected in MMIS or at an MCO for lack of authorization.

Req. ID #	Requirement Text	Requirement Type

Authorization Utilization Status

For authorization utilization status, a DHHR, MCO, or provider user can request the AuthentiCare Authorizations Report and select the option to Include Claim Details. This shows the user the total units authorized, the number of claims filed against the authorization, and the number of units still remaining in the authorization.

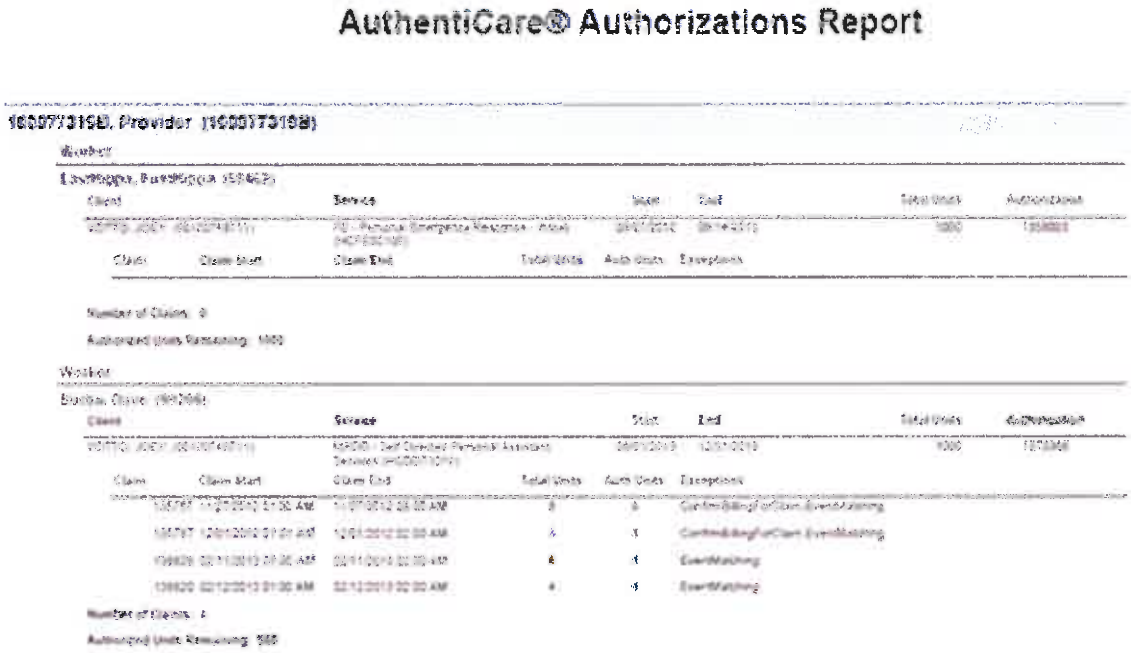


Figure 6.2 – Sample AuthentiCare Authorizations Report

Scheduling

Providers can access the AuthentiCare scheduling feature to schedule worker visits to recipients' homes. During the scheduling of a visit, the visit is tied to an authorization to seamlessly track the number of units available for use in each authorization. If a scheduled event exceeds the number of units available, AuthentiCare will notify the user that the number of units has been exceeded.

AuthentiCare compares the scheduled events to the actual check-in and check-out times of the worker and alerts the provider via email if a worker is late or if an event is missed. AuthentiCare also allows providers to schedule backup workers for events.

Visit Verification

First Data's AuthentiCare solution provides both integrated telephony and GPS enabled device technology. Our GPS application incorporates secure Store and Forward technology that enables visit capture when the mobile device does not have network (Wi-Fi/cellular) access. This gives DHHR care providers the flexibility to take advantage of the most appropriate technology for the individual situation of each care recipient and worker serving them and complies with 21st Century Cures Act EVV requirements. The service recipients and providers can use technology, such as their own existing phones to perform visit verification.

Visit information can be collected through an iOS or Android mobile app to confirm workers with the appropriate credentials are providing care at the correct locations, to the right consumer, for the approved services, and during the required timeframe. To validate service location, the AuthentiCare Mobile app uses iOS or Android GPS location services. Visit information can also be collected through an IVR system that collects the same information. IVR verifies the service location by using the Automatic Number Identification (ANI) similar to caller ID of the phone from which the worker is calling.

Req. ID #	Requirement Text	Requirement Type

Integrated GPS-enabled apps: AuthentiCare Mobile Application

The AuthentiCare solution provides an AuthentiCare Mobile application (available in the Apple Store and the Google Play Store for no charge). It uses the network time and GPS location services on these devices to verify the time and location of care delivery. The app tracks scheduled appointments and unscheduled visits, and provides fast, easy processing for a caregiver to check-in at the start of care and check-out when finished. The app uses a HIPAA-compliant, secure connection to an AuthentiCare web service portal to record visit activity when it has a connection to the internet, and stores encrypted visit data on the device for delayed transmission (store and forward) when there is no Wi-Fi or cellular data coverage. The app minimizes device GPS and data traffic to keep battery and data consumption low. (Data consumption is typically less than 50 MB per month for a worker doing 5 visits per week.)



Figure 6.3 – AuthentiCare Mobile App – iPhone

A configurable geo-fence is defined (based on State DHHR policy) around service location(s) stored on the client record. The app then verifies that the check-in and check-out locations lie within the client's geo-fence. In addition, the AuthentiCare Mobile app provides a number of key features to the DHHR's user community:

HIPAA-compliant security: All data on the device and in transit is Advanced Encryption Standard (AES) encrypted. The app requires two-factor authentication of users—login ID and device ID registration to the user.

Secure store and forward technology: For some states, up to 20 percent of care locations have no Wi-Fi or cellular data service at the indoor place of service. AuthentiCare allows the user to record time and GPS location of service in the app at the time and place service is delivered. The information is recorded in the online system when the worker carries the device to a location where they can connect to Wi-Fi or cellular data service. The iOS and Android apps have a page banner that turns red when there is no data connection or when the device is in airplane mode. The banner turns white when the device reestablishes a data connection so that the user can tell when data services are available.

"Learn Mode" coordinate refinement: The AuthentiCare web portal allows case managers or care coordinators to view client coordinates on a map, enter coordinates from a web application such as Google Maps, or update coordinates that are incorrect. It also provides a "learn mode" that uses actual coordinates recorded during care visits and a proprietary method to refine GPS coordinates on the client record.

Multiple language support: The standard AuthentiCare mobile app will support English and Spanish, and includes the ability to add extensions to support additional languages.

The AuthentiCare Mobile app has two modes: Standard and Frontier. Individual workers can be set up in AuthentiCare to use the mode that best fits the services they provide.

Standard Mode: The Standard mode of the AuthentiCare Mobile app is intended for use in situations where the worker will have Wi-Fi or cellular data connection most of the day, and particularly at the beginning and end of the day. This would typically be in-town users where cell coverage is good. The worker logs in each day with their registered iOS or Android device, and downloads a list of their appointments for the day. The worker then checks in and checks out for each visit during the day. If the worker is in an area with a data connection, their activity is pushed to the web portal in real time, and their provider home office can view the activity in the AuthentiCare web portal. If the worker does not have a data connection at the time and location of service, their activity is stored on the device, and the user receives periodic reminders to return to a location with data service to allow the device to record the activity in the portal.

Req. ID #	Requirement Text	Requirement Type

Frontier Mode: The Frontier mode of the AuthentiCare Mobile app is intended for use in situations where the worker lives and delivers services in an area with no Wi-Fi or cellular data service, and potentially even without electricity. In these cases, the worker can use a vehicle charger to keep their mobile device charged, and can use the mobile app store and forward technology to record up to seven days of activity before returning to a location with Wi-Fi or data service to upload their visit information. Since GPS service is a satellite-based technology, in most locations, even when cellular service is not available, the GPS coordinates can still be captured and stored, especially if the worker checks in or out from a front porch or other location with a sky view (working like satellite radio).The worker begins a cycle of up to seven days by going to a location with data service and downloading a list of scheduled appointments and a list of their assigned clients. The worker then can go to their remote location and enter check-in and check-out information as the worker provides service. Later on, the worker then returns to a location with cellular data or Wi-Fi service to allow the AuthentiCare Mobile app to record their stored visits and refresh their appointments and client list for the next cycle. Frontier mode users frequently do not purchase a data plan for their device and rely on a location with public Wi-Fi to refresh their device.



Figure 6.4 – iPhone – Frontier Mode with no Internet Connection

With the national trend toward phone companies eliminating support for land line or Wi-Fi Internet Protocol (IP) phone service in rural areas, due to the expense of maintaining their copper wire networks, the AuthentiCare Mobile app provides a robust EVV solution that can verify location of care, and is not dependent on wire networks.

Telephone: AuthentiCare Interactive Voice Response

For situations where there is a land line and the client has a phone in their home, the AuthentiCare solution's Interactive Voice Response system provides workers with an intuitive and user-friendly method of visit verification using a single toll-free number. Using the recipient's phone, landline or cellphone (depending on state policy), workers can call the IVR system to initiate service delivery via a check-in and check-out process from any service location.

Worker and Recipient Identification: During the IVR call, the Worker ID is collected to identify the worker (by name and ID) and the provider agency for which they work. The recipient is identified by matching the Automated Number Identifier from the call to the preregistered phone number of the recipient recorded within AuthentiCare. The IVR prompt scripts are configurable and available in English and Spanish. The phrasing will be tailored to the needs of the DHHR.

If the worker is checking out, the IVR also allows workers to enter a record of Plan of Care activities completed during the visit, as well as any observations of changes in the recipient's condition or issues with the plan of care meeting the recipient's needs.

AuthentiCare Web Claim Entry

For cases where the worker forgot to record service or had technical difficulties, providers or employers of record are able to retroactively enter the visit details on the AuthentiCare web site. Web entry does not provide visit verification. However, it does provide a means for providers to make additions or corrections to the record, or to enter claims for periodic services (for example, Financial Management Services [FMS] monthly service fee or Case Management phone contact) where there is no expectation of a visit to the client as part of the service. States frequently add other services to the AuthentiCare web system so Provider agencies can manage all of their related services in one place, and bill all of them through AuthentiCare.

Web entry is fully audited to make clear who entered the claim and when. AuthentiCare allows for one time claim entry and/or multiple visits at once through the Claim Express screens. The Claim Express filter page shows where the client, worker, and service information is entered by the provider for whom they are intending to enter visits. The Claim Express grid shows where multiple dates of service and times can be entered by the provider at once. This could be 10+ visits (there is not a limit to the number of visits rows that are available) from a time card that the worker filled out. When complete, the provider can save all of the visit/claim information at once.

Req. ID #	Requirement Text	Requirement Type

Billing

The AuthentiCare SaaS solution incorporates FWA detection and prevention into a work flow process for providers known as a "claim scrub" process. If the worker uses EVV properly, the documented visit travels through the process and can be automatically billed with minimum intervention by the provider. If the workflow detects issue(s) with the visit documentation, the claim is flagged with a critical exception for the provider to "scrub" and make corrections before it can be billed. The following is a diagram of the process.

"Claim Scrub" Process

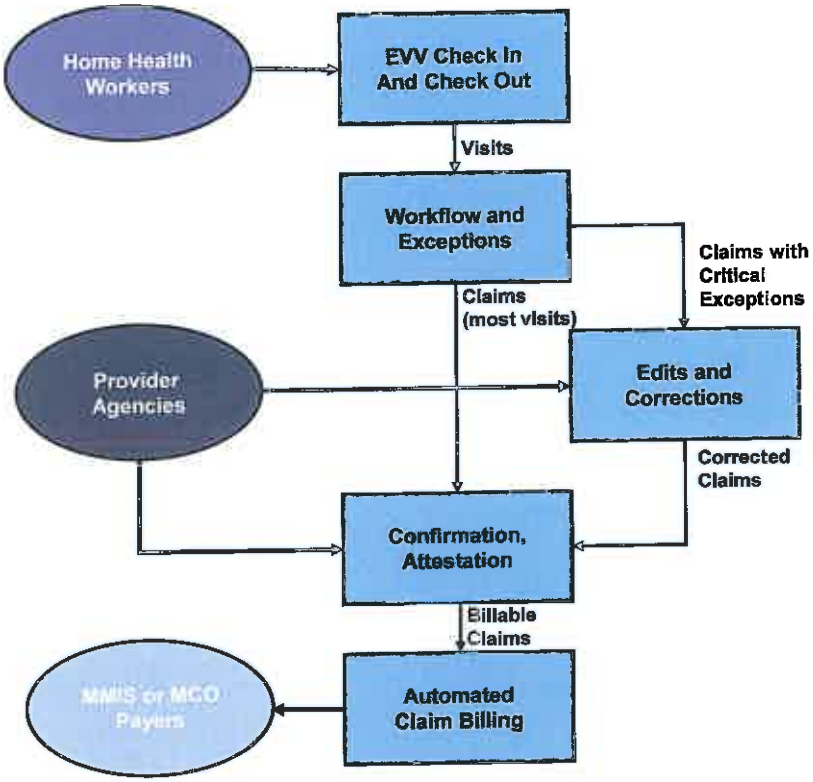


Figure 6.5 – Claim Scrub Process Flow

The "claim scrub" process has five main steps:

1. **EVV Check-in and Check-out**: The caregiver documents the visit to the recipient by checking in and out at the beginning and end.
2. **Workflow and Exceptions**: AuthentiCare examines the visit documentation according to configurable business rules and creates a claim that may have one of two types of exceptions:
   - Critical Exceptions: Issues such as missing a checkout or missing an authorization are critical and prevent a claim from being billed.
   - Informational Exceptions: Issues such as care occurred in an unauthorized location that are flagged for reporting and investigation, but not usually used to prevent billing.

Visits with critical exceptions are held in the system for the provider to review and make corrections, while those with no exceptions or only informational exceptions are staged for provider approval.

3. **Edits and Corrections**: AuthentiCare makes it easy for Providers to address errors and exceptions. The system provides an Exception Dashboard that breaks critical exception visits (those that are currently non-billable) into separate categories for any date of service range.

Clicking on a list button takes the provider to a summary list of visits with that exception for the provider to drill down

Req. ID #	Requirement Text	Requirement Type

and make corrections.

4. **Confirmation and Attestation**: For "clean" visits, providers are required to confirm and attest that the caregiver visits are correct and appropriate for billing. This gives the provider's final approval for billing on the provider's behalf. Providers can approve on a visit by visit basis or use a web summary view. Providers can also schedule an overnight automated process.
5. **Automated Billing**: AuthentiCare incorporates an ANSI X12 standard EDI process for billing confirmed visits. This process automatically routes the claims to MMIS or to the MCO that the recipient is enrolled with, based on the payer that issued the authorization for service and agreed to pay for it. In most states this process runs on weekdays, so providers control the timing of their submissions by controlling when they complete confirmation.

Once the providers and workers are accustomed to EVV and using it routinely, providers see two major benefits from using the system for claims and "claim scrub":

- **Minimizes administrative work**: AuthentiCare eliminates timesheets and checklists and administrative work to process them. Most visits are captured cleanly from EVV so the provider only has to approve them.
- **Provides no fee billing service**: Many providers are paying an independent biller or clearinghouse a per claim fee to format and submit claims to MMIS or to the MCOs. AuthentiCare provides claim submission as a no fee service.

VV018	The solution should verify visit components are within program requirements when a visit verification service is initiated and ignore, warn, or stop the user from entering data into the solution as determined by Department.	Visit Verification

AuthentiCare provides a mature, robust EVV solution that captures visit verification data as required by business rules and edits from DHHR. We use data capture methods like drop-down lists and validation edits based on DHHR program requirements and business rules to maintain data integrity for all visits. Informational, warning, and error messages are presented to the user depending on the data entered. Depending on the scenario, error situations will prevent the user from entering invalid data. All message text and triggers will be reviewed with DHHR during the iterative design sessions.

VV019	The solution should securely capture an independent verification of the service delivery from the member receiving services.	Visit Verification

AuthentiCare mobile and IVR solutions support recipient attestation to view a summary of the service performed and attest to the service delivered by approving or rejecting the summary of the service provided. This feature can be enabled at the service level allowing for maximum flexibility on its required usage. The recipient can attest to the service provided by using an e-signature or voice biometrics within the mobile application.

VV020	The solution should have the ability to allow a direct care worker and/or provider agency to record visits to multiple members within a 24 hour period.	Visit Verification

AuthentiCare allows multiple caregivers and/or agencies to provide services to a client on the same day, either at the same time or at different times that day. This frequently happens when a Case Manager checks in while personal care or companion services are being rendered. Some Case Managers use the real-time information in AuthentiCare deliberately check in during delivery of services to witness care being provided. The two visits remain completely independent in AuthentiCare so each person performs check-in and check-out normally. AuthentiCare provides an Overlapped Claim by Client Report that allows Providers, Payers, and State employees to distinguish between overlaps that are normal and overlaps that may indicate an issue.

It is common for a personal care worker, nurse, or Case Manager to visit multiple clients in a day. Both the AuthentiCare IVR and Mobile App allow the caregiver to select the service recipient for each individual visit.

AuthentiCare is configurable so DHHR can determine the business rules for multi-service visits as well as visits to multiple members within a 24-hour period.

VV021	The solution should account for living arrangements in which multiple members receiving services reside at a single address.	Visit Verification

Both the AuthentiCare IVR and Mobile App present a list of authorized clients in the caregiver's location for the caregiver to select who they are serving. Figure 6.6 displays a sample screen where multi-client visit details may be captured.

The caregiver selects the first client receiving service and the associated services. In the mobile app, the caregiver can then select "Add a Client" and select the services associated with that client. The IVR will prompt, "If you are finished selecting clients and services, press 1. If you want to add an additional client, press 2." Once the selection process has

Req. ID #	Requirement Text	Requirement Type

been completed, the caregiver selects Check-in on mobile or '1' on the IVR.

This enables the caregiver to check in quickly for multiple clients in a single visit.



Figure 6.6 – Mobile display for capturing Multi-Client Visit Details

VV022	The solution should have the ability to allow multiple direct care workers and/or provider agencies to record visits to a member within a 24 hour period.	Visit Verification

AuthentiCare also supports the ability to record and verify multiple services/transactions within one EVV visit. Frequently, workers provide personal care for a period of time, and then provide companion services for additional time. Most states want the worker to check out from the first service and check in for the second so they know how much time of the visit to allocate to each service. There are other states where the authorization sets a time allocation rule between the two services, so the worker can check in at the beginning and check out in the end, and have the system allocate the time between the two services. Some workers do not like having the system allocate time because if the personal care takes longer on a given day, the worker can get paid less. This is why most states prefer to have the worker check out for the first service and check in for the second.

AuthentiCare is configurable so DHHR can determine the business rules for multi-service visits as well as visits to multiple members within a 24-hour period.

VV023	The solution should have the ability to account for situations in which services are provided to a group of members during a single visit.	Visit Verification

The Mobile App (and IVR optionally) present a list of authorized recipients in the worker's location for the worker to select who they are serving. When the worker wants to serve another recipient, they can check out and then select the other recipient to check in. AuthentiCare supports multi-client check-in and check-out. Examples include teaching two or three people how to shop, or how to do rehabilitative tasks at the same time.

VV024	The solution should have the ability to account for situations in which the member and the direct care worker reside at the same address.	Visit Verification

AuthentiCare supports this scenario where both the member and DCW reside at the same address.

This scenario happens frequently in Self-Directed care. In most cases the worker can simply check-in and out at the beginning and end of their shift and indicate on a checklist what tasks were done. AuthentiCare has an optional Representative (Employer) portal where an Employer of Record (EOR) can obtain time records for their workers to

Req. ID #	Requirement Text	Requirement Type
meet FLSA requirements. The EOR can also set up email alerts for when care begins and ends.		
VV025	The solution should account for situations in which a visit starts and/or ends away from the member's place of residence.	Visit Verification
AuthentiCare supports visits that begin and end at different locations. EVV data are captured regardless of location. The system does not prevent check-in or check-out, but exceptions can be configured. DHHR can determine if this is an exception that should prevent visit submission (Critical) or if it should not prevent visit submission (Informational). Adult Day Care or Non-Emergency Transportation services frequently use this feature for regular appointments and visits AuthentiCare supports registration of an unlimited number of recipient addresses with GPS locations or recipient landline phone numbers, all of which can be used for location verification. Exception processing as noted above is available based on DHHR business rules.		
VV026	The solution should be configurable to either allow or prevent multiple direct care workers and/or provider agencies from providing services to a member at the same time.	Visit Verification
AuthentiCare supports the configuration of unique business rules at multiple levels including by service provided. It can thus be configured to either allow or prevent multiple direct care workers and/or provider agencies from providing services to a member at the same time.		
VV027	The solution should verify that the agency providing the service has a valid pre-authorization for each member served on file.	Visit Verification
Providers can use AuthentiCare to schedule workers' visits to recipients' homes. A scheduled visit is called an event. Each event must be linked to an authorization. Events may only be scheduled for authorized client/service/provider/worker combinations. AuthentiCare tracks the number of units available for scheduling in each authorization and notifies the scheduler if an event exceeds the number of units available for scheduling. AuthentiCare notifies the provider with an alert, and offers choices of discard, accept, or change the scheduled event if the client or worker have been previously scheduled for that timeframe. AuthentiCare also allows providers to schedule back-up workers for events. AuthentiCare compares the scheduled events to the worker's actual check-in and check-out and alerts the provider via email if a worker is late or if an event is missed. If a worker is scheduled for an event on a regularly occurring day off, AuthentiCare displays a warning message alerting the scheduler to this conflict. The scheduler may choose to change the event or to save it although there is a conflict. AuthentiCare schedule warnings are designed to assist schedulers, but not prevent the scheduling an event with a conflict.		
VV028	The solution should verify that the time of the visit is within the parameters outlined on the prior authorization and recorded in a format that can be sorted. The format should be YYYY-MM-DDTHH:MM:SS or equivalent.	Visit Verification
Dates within AuthentiCare are stored in Microsoft SQL date format and can be sorted. Visit dates are compared to dates on the associated authorizations and exceptions are applied as appropriate to prevent billing submission for services provided that are not within the authorization timeframe. Please see VV032 for additional details.		
VV029	The solution should have the ability to allow the Department to identify circumstances in which visit verification is not necessary.	Visit Verification
AuthentiCare's flexible, configurable platform allows the Department the ability to identify when visit verification is mandatory, optional, or simply not required. For example, AuthentiCare supports check-in only services that capture delivery time and location for things like Home Delivered Meals to verify the delivery was really there, but not necessarily the length of time the person was there. Additionally, our solution supports periodic or one-time services like Monthly FMS fees or PERS Installation, so that the services are managed and billed through the same EVV system as is used to manage Personal Care. Providers can see and report on all their claim information in on place and Case Managers can see all of the services a client receives in one place.		
VV030	The solution should send real-time alerts when a visit documented in the prior authorization system is not initiated at the scheduled time.	Visit Verification
AuthentiCare delivers the ability to configure automated alerts, like when services are late or missed, so a qualified back-up worker may be dispatched. Automated alerts may be sent via email to designated recipients as determined by DHHR policy. Support coordinators, provider agencies, emergency back-up workers, or State staff may be notified that a critical service has not been delivered.		

Req. ID #	Requirement Text	Requirement Type
Alerts may also be configured to meet the requirements of individual services or programs as DHHR chooses, and alerts can go to multiple recipients as defined in the template. These alerts can be tracked by caregiver, provider, or recipient in various reports and dashboards to identify trends that need to be addressed.		
VV031	The solution should have the ability to account for circumstances in which a visit crosses calendar days.	Visit Verification
The AuthentiCare IVR and Mobile App capture the date and time of both check-in and check-out, so service can continue over midnight as with Sleep Cycle Support. Per MMIS rules, the date of service for the service on the billed claim is normally the date on which the service starts. Another available option is to break visits that span calendar days into two separate visits with two different dates of service.		
VV032	The solution should accommodate different definitions of pending, late, and missed visits by the status types as defined by the applicable program and/or waiver service.	Visit Verification

AuthentiCare delivers the ability to configure automated alerts, like when services are late or missed, so a qualified back-up worker may be dispatched. Automated alerts may be sent via email to designated recipients as determined by DHHR policy. Support coordinators, provider agencies, emergency back-up workers, or state staff may be notified that a critical service has not been delivered.

Users can also configure alerts to meet the requirements of individual services or programs as DHHR chooses, and alerts can go to multiple recipients as defined in the template. These alerts can be tracked by caregiver, by provider, or by recipient in various reports and dashboards to identify trends that need to be addressed.

The timeframe for defining when a visit is considered late or missed is easily configurable. For some services, the Department may want to mark a visit as late at 15 minutes past the scheduled start time, and self-directed or other services may want to have a longer or shorter tolerance level. The DHHR decisions will be defined through the iterative design sessions and documented in the Configuration and SIP documents as well as in User Manuals. The template in Figure 6.7 is used by administrative staff to customize the message text of the email. This allows custom messages to be created while confirming that the privacy and security of Protected Health Information is maintained. To meet HIPAA security and privacy rules, beneficiary information normally cannot be included in the alert. However, the alerts do include a link to the appointment in AuthentiCare so that the individual receiving the alert can be directed to the exact appointment that is late or missed. Figure 6.7 also shows how late and missed visit thresholds can be adjusted and how the email templates can be modified:

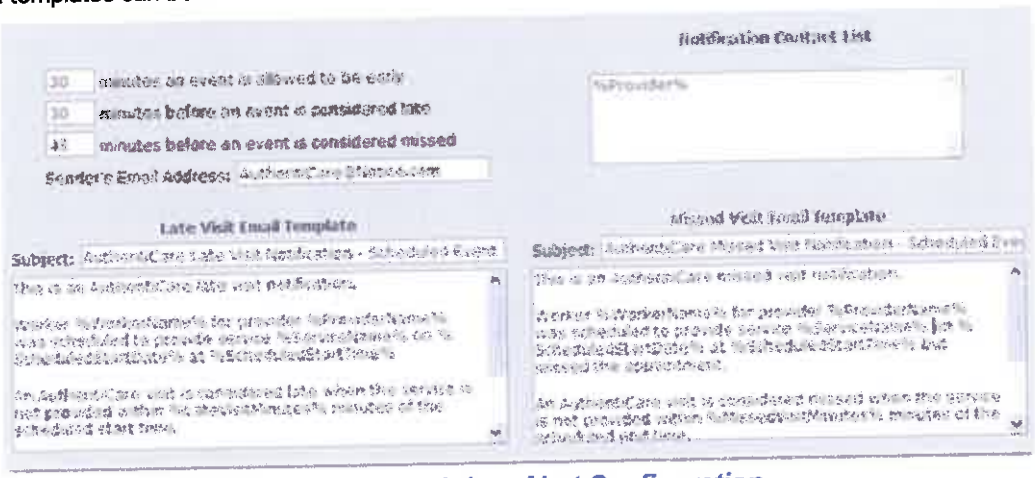


Figure 6.7 – Real-time Alert Configuration

To prevent "alert fatigue," it is critical to define timing and escalation of the alerts to maximize the meaning of an alert when it is received, and minimize the number of false alarms. AuthentiCare alert thresholds can use statewide default values or specific values for a type of service. Optionally, there can be special values for specific critical recipient needs, like for at-risk recipients. Alerts can be disabled for some services (for example, services that are not scheduled, or unit-based services like Home Delivered Meals), or for situations where the recipient is in a remote "no tech zone" where the visit data will be submitted by Store and Forward from the Mobile App at a later time. These options reduce false alarms. Automated alerts are sent via email to designated recipients. Support coordinators, provider agencies, emergency back-up workers, or state staff may be registered to be notified that a critical service has not been delivered. For example, AuthentiCare can be configured so that only providers receive late alerts whereas

Req. ID #	Requirement Text	Requirement Type
Care Managers, state staff, or others could be notified of missed alerts only. AuthentiCare is easily configurable to set up multi-level escalating alerts for late or missed visits as needed by DHHR.		
VV033	The solution should allow a direct care worker and/or provider agency to receive messages indicating a possible problem with a visit verification.	Visit Verification
AuthentiCare reduces fraud, waste, and abuse by subjecting every visit to a pre-billing business rules evaluation workflow that applies exceptions and prevents providers from billing for incomplete or unauthorized services, preventing compliance issues before they occur. The DCW or provider agency may receive an alert/message noting a possible problem with a specific visit verification. AuthentiCare examines the visit documentation according to configurable business rules and may create one of two types of exceptions: • **Critical Exceptions:** Issues like missing a check-out or missing an authorization are critical and prevent a claim from being billed. • **Informational Exceptions:** Issues like care occurred in an unauthorized location that are flagged for reporting and investigation, but not usually used to prevent billing. Claims with critical exceptions are held in the system for the provider to review and correct, while claims with no exceptions or only informational exceptions are staged for provider approval. AuthentiCare makes it easy for providers to address errors and exceptions that do occur. The system provides an Exception Dashboard that breaks critical exception claims (claims that are currently non-billable) into separate categories for any date of service range. Clicking on a list button takes the provider to a summary list of claims with that exception for the provider to drill down and make corrections. The workflow and its administrative web applications allow FDGS to configure business rule options to control how claims are verified and exceptions are applied. This in turn determines how claims are ultimately billed. Working with our customers and their waiver and non-waiver rules, AuthentiCare maintains a library of configurable workflow plug-ins that encompass the most common Medicaid business rules for processing visits.		

6.2 Program Management

RFP Section Attachment 7 – 3-3.1 & 4.4.1.2, pp. 117, 51
3. Program Management
3.1 Refer to the relevant business specifications located in Appendix 1: Detailed Specifications and pertinent narrative in Section 4: Project Specifications in this RFP to cover solution capabilities in this area. The Vendor should describe its approach to Program Management below. The narrative response for this category should be organized using the appropriate subject matter area as per Appendix 1: Detailed Specifications.

This sub-section describes our approach to Program Management. AuthentiCare provides DHHR, your providers, and your beneficiaries with a flexible set of technical options to capture and verify the required information for each visit, including the time, location, and task(s) performed during service delivery. FDGS provides additional detail in this sub-section to meet the mandatory requirements listed in Table 6.4 as part of RFP Attachment 6 – Mandatory Requirements.

Table 6.4 – AuthentiCare Meets all Mandatory Requirements for Program Management

Met	Req ID #	Requirement Text
☑	MR001	All provided services must comply with the Department rules.

AuthentiCare employs a modular, flexible approach to systems development, including the use of open interfaces and exposed application programming interfaces (APIs) to separate business rules from core programming. This makes our AuthentiCare solution highly modular, extensible, interoperable, and flexible to support the EVV program in West Virginia. Table 6.5 details how AuthentiCare will meet each of the Program Management requirements from Appendix 1 of the RFP.

Table 6.5 – Detailed Response to Program Management Requirements

Req. ID #	Requirement Text	Requirement Type
PG001	The solution rules/procedures should allow and enforce multiple service limits for different service ranges including, but not limited to:	Program Management
PG002	Day	Program Management
PG003	Week	Program Management
PG004	Month	Program Management
PG005	Year	Program Management
AuthentiCare supports the application of unique rules and edits to enforce multiple service limits and different service ranges including day, week, month, and year. Additional range values will be discussed and evaluated during the iterative design sessions early in the implementation period.		
PG006	The solution rules/procedures should accommodate retroactive prior authorizations and changes to prior authorizations based on revisions to recipients' plans of care/service plans.	Program Management
AuthentiCare accommodates retroactive prior authorizations and changes to prior authorizations based on revisions to recipients' plans of care/service plans. The AuthentiCare website provides an easy-to-use interface for providers to search and view all authorizations.		
PG007	The solution should have the ability to round service delivery time.	Program Management

Req. ID #	Requirement Text	Requirement Type
AuthentiCare includes the options to round service delivery time according to DHHR policy. AuthentiCare offers several rounding options (standard, round up, round down) with most states choosing standard rounding because workers usually view it as the fairest option.		
PG008	The solution should provide a master client index of client information, including a single unique identifier (that is not the Social Security Number), for all clients.	Program Management
AuthentiCare assigns clients a unique Client ID when imported or entered into the system, including a single unique identifier (that is not the SSN).		
PG009	The solution should maintain an integrated repository of provider agency information, including a single unique identifier, for all providers.	Program Management
AuthentiCare also maintains a fully integrated data repository of provider agency details. The provider agency and each provider (DCW) is assigned a unique identifier.		
PG010	The solution should be able to capture, verify, and support billing for in-home and community based setting service visits.	Program Management
AuthentiCare inherently supports the capture, verification and billing for all service types and related visits. We will configure AuthentiCare specifically to meet DHHR program policies for Personal Care Services (PCS) and all in-home and community-based service settings.		
PG011	The solution should have the ability to create Health Insurance Portability and Accountability Act (HIPAA)-compliant electronic 837 claim file submission to the State MMIS for claims processing in compliance with all Medicaid filing requirements.	Program Management

AuthentiCare incorporates an ANSI X12 standard EDI process for billing confirmed claims. This process automatically routes the claims to the MMIS. FDGS creates and submits both 837P and 837I for states today in compliance with all Medicaid filing requirements.

AuthentiCare's integration capabilities are based entirely on open-systems standards and accommodate communications to database management systems and back-end solutions through APIs and custom imports and exports. Additional features, like Microsoft's BizTalk EDI 837 file creation, are built into the AuthentiCare solution and leverage the open standard architecture. AuthentiCare's feature-rich solution supports MITA's seven conditions and standards.

Our proposed AuthentiCare team is familiar and experienced in working with different state agencies with multiple vendors. For example, for the Nevada implementation, coordination with DXC for interfaces was essential to receiving provider and member data, and our staff was able to work with all MCOs to facilitate authorizations and 837/835 integration.

We have successfully built and continue to maintain interfaces to DXC-managed, and other state MMIS systems. Further, we have a successful record of submitting claims at a high rate of accuracy. As part of our integration into MMIS systems from various states, 99.4 percent of first-pass claims submitted from AuthentiCare to their system paid successfully, resulting in less post-adjudication adjustments and rework. We anticipate having the same type of success integrating into the West Virginia MMIS and related systems for provider claims submissions and similar data exchanges.

Currently, AuthentiCare is integrated with DXC-operated and managed MMIS systems in:

- Oklahoma (DXC/interChange): Since beginning our operation in 2009, AuthentiCare has processed 4 million claims annually for more than 300 provider locations and 26,000 beneficiaries. 99.5 percent of submitted claims were transmitted and paid via an 837 specification compliant file to the DXC MMIS portal.
- Kansas (DXC/interChange): Since 2010, AuthentiCare has processed 4 million claims annually for more than 600 provider locations and 21,000 beneficiaries. 99.3 percent of submitted claims were transmitted via an 837 specification compliant file to the DXC MMIS portal for adjudication.
- Alabama (DXC/interChange): AuthentiCare went live on October 1, 2017. Since then, over 5 million claims have been processed, and 837 and 835 files are being exchanged via secure File Gateway with the DXC operated and managed MMIS system. 98.9 percent of claims submitted to the DXC MMIS portal were successfully paid.

PG012	The solution should automatically generate all required correspondence to individuals.	Program Management

AuthentiCare does not support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements once Phase 1 has been successfully implemented.

Req. ID #	Requirement Text	Requirement Type
PG013	The Vendor should provide correspondence metric reports upon request by the Department.	Program Management
AuthentiCare does not support automated generation of forms or correspondence nor related metric reporting specific to correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements once Phase 1 has been successfully implemented.		
PG014	The solution should assist users in identifying which sections of forms should be filled in manually.	Program Management
AuthentiCare does not support automatic forms generation or auto-fill functionality. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements once Phase 1 has been successfully implemented.		
PG015	The solution should provide the ability to deliver reports as mutually agreed-upon with the Department.	Program Management

The main reports engine web page provides easy access to run on-demand reports, as well as to create and schedule regular reports for re-use, and then pick up completed reports in the user's preferred format (including PDF, Excel, CSV, and XML). The system allows the user to schedule or submit report requests, do other work while the report(s) run, and then come back to the page to pick up the report(s) when they are ready.

Additional reports are added to the AuthentiCare list of Standard Reports as enhancements are made to the core product over time. FDGS will work with DHHR to identify unique reporting requirements and delivery options.

Table 6.6 – AuthentiCare Standard Reports

Report Name	Report Description
Authorizations	Lists all authorization details
Authorization History	Gives authorization history and highlights new or changed authorizations
Authorizations w/ Claim Details	Lists authorization details and associated claims information. Therefore, this report gives the user authorization utilization information
Billing Invoice	List of claims by service date and export/submission date, along with the billing status and amount
Calendar	Lists all scheduled events
Claim Data Listing	Lists, by provider and worker, all services performed during a given time period and the total dollars billed to and paid by MMIS
Claim Details	Claim listing with details that can be grouped by beneficiary
Claim History	Reports all claim activities by referencing claim audit data
Eligible Client Data Listing	Lists beneficiaries a provider is eligible to serve and information on each beneficiary such as address, phone number, and Medicaid ID
Exception	Lists claim exceptions, as defined in the AuthentiCare workflow
Late and Missed Visits	Details late and missed visits and any selected reason codes
Overlapped Claim By Client	Identifies beneficiaries that have two workers providing care at the same time
Overlapped Claim By Worker	Identifies workers who are servicing two beneficiaries at the same time
Provider Activity	Lists services performed during a given time period and the total dollars billed to MMIS (or MCO), by worker

Req. ID #	Requirement Text	Requirement Type
Remittance Advice	Details remittance advice status, allowing providers to examine paid claims and reconcile payment amounts	
Remittance Data Listing	Lists, by provider, all remittance records (payments and denials) so that the provider can examine paid claims and reconcile payments	
Time and Attendance	Reports check-in and out times	
Unauthorized Location	Highlights mobile app visits recorded from an unauthorized GPS location	
Unauthorized Phone Number	Highlights IVR calls made from an unauthorized phone	
Worker Activity	Displays check-in/out times only and no billing information. Also displays any claim notes	
PG016	The solution should provide flexible web-based reporting, including ad hoc reporting of all data stored within the solution.	Program Management
The AuthentiCare Web Application includes a robust reporting engine for use in EVV program monitoring and management, and to help identify and reduce fraud, waste, and abuse. AuthentiCare contains a broad spectrum of on-demand reports that contain ad hoc functions like drop down list filters, parameters, date ranges, and other selections that allow users to report the data of which they are specifically interested. This allows DHHR and providers the ability to search through summary and detailed data views. Using selection criteria for each report, a user can customize the standard report to meet specific requirements easily and simply, and run a one-time report, or save a report that they want to run regularly for ongoing analysis or metrics submissions. These reports provide DHHR stakeholders, as well as the provider community (based on their security access authority), views into the electronic visit and verification data to manage the programs, confirm beneficiaries receive needed care, and help identify fraud, waste, and abuse. FDGS will work with DHHR reporting needs, and will confirm that any additional reporting needs are met through joint requirements discussions with the Department.		
PG017	The solution should have the ability to make a complete set of data related to visits submitted for verifications available for reporting, including, but not limited to the following elements:	Program Management
PG018	Member receiving services	Program Management
PG019	Direct care worker	Program Management
PG020	Provider	Program Management
PG021	Location of visit	Program Management
PG022	Date of visit	Program Management
PG023	Start time of visit	Program Management
PG024	Missed visits	Program Management
PG025	Late visits	Program Management
PG026	End time of visit	Program Management
PG027	Visit late time	Program Management
PG028	Services provided	Program Management

Req. ID #	Requirement Text	Requirement Type
PG029	Manual or electronic verification	Program Management
FDGS confirms that AuthentiCare compiles all EVV data, including all data elements listed in PG018 – PG029, into a complete set of data related to visits submitted for verifications. The AuthentiCare database and all data elements are available for reporting, role-specific dashboards, and export.		
PG030	The solution should have the ability to use identifiers, mathematical functions, formatting, and manipulate data within reports	Program Management
AuthentiCare report data are available in Excel, CSV, PDF, and XML and can be extracted by state staff, MCOs, providers, and other authorized users to merge with existing data for additional report design and generation.		
PG031	The solution rules/procedures should have the ability to ensure the direct care services do not overlap with other direct care services.	Program Management
AuthentiCare supports the ability to edit direct care services to avoid overlap with other direct care services. Currently, AuthentiCare allows multiple caregivers and/or agencies to provide services to a client on the same day, either at the same time or at different times that day. This frequently happens when a Case Manager checks in while personal care or companion services are being rendered. Some Case Managers use the real-time information in AuthentiCare to deliberately check in during delivery of services to witness care being provided. The two visits remain completely independent in AuthentiCare so each person performs check in and check out normally. If additional edits are not added to AuthentiCare, it already provides an Overlapped Claim by Client Report that allows Providers, Payers, and State employees to distinguish between overlaps that are normal and overlaps that may indicate an issue.		
PG032	The solution should compile information from all EVV data sources and calculate total daily and weekly hours worked by direct care workers and agencies.	Program Management
AuthentiCare is designed to validate that beneficiaries are receiving authorized services according to their care plans in home or facility settings, while automating worker timekeeping and compliance with Fair Labor Standards Act (FLSA) records requirements. It will compile work hours to calculate total daily and weekly hours by DCW and agency. Our solution includes a set of modules for scheduling and appointments, time and attendance tracking, claim creation and editing, billing, and reporting that can be configured to meet the business rule requirements of different Medicaid-related programs and waivers.		
PG033	The solution should have the ability for the Department to allow and/or not allow retroactive care plan changes for specific services and/or programs through a configurable interface.	Program Management
AuthentiCare supports authorizations that arrive after care has been provided. Visits can be held within AuthentiCare through the exception process until matched with the prior authorization. This helps avoid rejection of the claim when submitted for payment by verifying service has been approved.		
PG034	The solution should allow the Department to define and limit the circumstances in which a manual verification can be made	Program Management
AuthentiCare offers options to restrict the ability to complete manual verifications even further. Please see PG006 for more details regarding manual verification of visits. AuthentiCare does not support Care Management specifically.		
PG035	The solution should use eligibility data transferred from the Medicaid Management Information System (MMIS) to determine if any waiver requirements apply. If no waiver requirements apply, the solution should assume that state plan requirements specific to the service being provided apply.	Program Management
AuthentiCare will be modified to accept eligibility data from the West Virginia MMIS to gather the applicable waiver requirements. Business rules will be added provide for any unique processing requirements under each waiver, if applicable. FDGS has integrated state waivers in other states. The workflow and its administrative web applications allow the AuthentiCare team to configure business rule options to control how claims are verified and exceptions are applied. This in turn determines how claims are ultimately billed. Working with our other AuthentiCare customers and their waiver and non-waiver rules, we have built a library of configurable workflow plug-ins that encompass the most common Medicaid business rules for processing visits. AuthentiCare does not support Care Management specifically.		

Req. ID #	Requirement Text	Requirement Type
PG036	The Vendor should review the Department waivers and other state plan program requirements to develop and propose system edits that will meet the need of the Department. The Vendor should propose system settings for the Department to consider during the initial solution configuration and during operations. The review and proposal process should happen at an interval defined by the Department.	Program Management
FDGS agrees to review the Department waivers and other state plan program requirements upon award. Similar to PG035, we have worked with our other AuthentiCare customers to properly apply rules and edits according to their waiver and non-waiver rules. As part of our implementation approach, waiver rules will be verified during our iterative design sessions. At the end of each project milestone, the updated AuthentiCare functionality will be demonstrated to the Department prior to the conclusion of each project milestone.		
PG037	The Vendor should provide web portal functionality that addresses the needs of:	Program Management
PG038	Provider agencies and their direct care workers	Program Management
PG039	Members	Program Management
PG040	Waiver program and/or legal representatives	Program Management
PG041	State program staff	Program Management
The AuthentiCare solution for EVV is deployed in both a web portal and mobile application that provides full functionality to provider agencies, direct care workers, and state program staff. While some additional functions, like reporting and administrative features, are only on the web, the free AuthentiCare mobile application provides all the functionality to securely gather the required EVV data in support of the 21st Century Cures Act and the DHHR EVV program and policies. FDGS will discuss with the Department future features, functions, and use cases as AuthentiCare enhancements addressing the needs of members, waiver programs, and/or legal representatives.		

6.3 Program Integrity

RFP Section Attachment 7 – 4.4.1 & 4.4.1.3, pp. 118, 51
4. Program Integrity
4.1 Refer to the relevant business specifications located in Appendix 1: Detailed Specifications and pertinent narrative in Section 4: Project Specifications in this RFP to cover solution capabilities in this area. The Vendor should describe its approach to Program Integrity below. The narrative response for this category should be organized using the appropriate subject matter area as per Appendix 1: Detailed Specifications.

This sub-section describes our approach to Program Integrity. FDGS has been developing and operating EVV solutions for 17 years in the Home and Community Based Services (HCBS) sector to address payment accuracy, enhance program integrity, and improve quality of care. FDGS is a leader in this industry having successfully implemented AuthentiCare for multiple states in programs using fee-for-service and managed care, provider agency and consumer-directed service delivery, offering various disbursement strategies integrated with diverse fiscal agents.

Table 6.7 – Detailed Response to Program Integrity Requirements

Req. ID #	Requirement Text	Requirement Type
PI001	The solution should have the ability to verify the delivery of electronic visit verification (EVV) services for multiple programs with different rules and edits.	Program Integrity
AuthentiCare's flexible framework supports any number of programs and related services with unique rules and edits to support different business rules and processes according to the DHHR EVV program policies. With a mature EVV solution, DHHR gains experience and policy knowledge from a team that has been developing and deploying EVV solutions since 2002.		
PI002	The Vendor should provide a summary of direct care workers and/or provider agencies who demonstrate a high level of missed and late visits, potentially fraudulent services, or potentially fraudulent billing patterns monthly and as requested by the Department.	Program Integrity

AuthentiCare can provide a summary of direct care workers and/or provider agencies who demonstrate a high level of missed and late visits, potentially fraudulent services or potentially fraudulent billing patterns through the AuthentiCare robust reporting engine for use in EVV program monitoring and management to help identify and reduce fraud, waste, and abuse. AuthentiCare contains a broad spectrum of on-demand reports that contain ad hoc functions like drop-down list filters, parameters, date ranges, and other selections that allow users to report the data of which they are specifically interested.

AuthentiCare combines data integrity edits and rules, reporting, and exception processing together to identify direct care worker practices and trends. With the maturity of our solution, DHHR gains years of fine tuning to enhance the prevention of fraudulent practices and the identification of potentially fraudulent billing patterns and other risky practices. Reports are available on-demand and through the exception dashboard described below.

AuthentiCare reduces fraud, waste, and abuse by subjecting every visit to a pre-billing claim engine workflow that applies exceptions and prevents providers from billing for incomplete or unauthorized services, preventing compliance issues before they occur.

AuthentiCare examines the visit documentation according to configurable business rules and may create one of two types of exceptions:

- **Critical Exceptions:** Issues like missing a check-out or missing an authorization are critical and prevent a claim from being billed.
- **Informational Exceptions:** Issues like care occurred in an unauthorized location that are flagged for reporting and investigation, but not usually used to prevent billing.

Claims with critical exceptions are held in the system for the provider to review and correct, while claims with no exceptions or only informational exceptions are staged for provider approval.

AuthentiCare makes it easy for providers to address errors and exceptions that do occur. The system provides an Exception Dashboard that breaks critical exception claims (claims that are currently non-billable) into separate

Req. ID #	Requirement Text	Requirement Type
categories for any date of service range. Clicking on a list button takes the provider to a summary list of claims with that exception for the provider to drill down and make corrections. The workflow and its administrative web applications allow FDGS to configure business rule options to control how claims are verified and exceptions are applied. This in turn determines how claims are ultimately billed. Working with our customers and their waiver and non-waiver rules, AuthentiCare maintains a library of configurable workflow plug-ins that encompass the most common Medicaid business rules for processing visits.		
PI003	The solution should track the time, location, and task performance of direct care workers during service delivery in order to safeguard against fraud, as well as to improve service delivery and program oversight.	Program Integrity
FDGS confirms that time, location, and task performance of direct care workers during service delivery is tracked in AuthentiCare. We already include alerts, exceptions, and reports to minimize and avoid fraud, waste, and abuse within the EVV and overall Medicaid program. The AuthentiCare team will work with DHHR to identify best practices and additional data to provide leadership with the decision-making knowledge needed to improve service delivery and focus its program oversight.		
PI004	The solution rules/procedures should have the ability to ensure the same direct care worker is not providing services to multiple recipients at the same time at different locations.	Program Integrity
AuthentiCare supports this scenario with the Master Worker ID, a unique statewide identifier that is used in identifying overlapping claims that may cross different provider agencies. The Master worker ID and associated reports have supported our clients' investigations into suspect bad actors and potential fraudulent behavior.		
PI005	The solution should have the ability to provide role-based reporting to review, analyze, and report all data across categories on a monthly basis and as requested by the Department, including, but not limited to:	Program Integrity
PI006	Payers	Program Integrity
PI007	Programs	Program Integrity
PI008	Provider Agency	Program Integrity
PI009	Direct Care Workers	Program Integrity
PI010	Members	Program Integrity
AuthentiCare is able to provide role-based reporting across all categories of data within the EVV solution. Roles and categories include Payers, Programs, Provider Agency, Direct Care Workers, Members, and more. At the EVV application level, the AuthentiCare solution is configurable for any number of roles and rights combinations. However, in our experience, most of the default provider roles and their accompanying rights are sufficient for most implementations. We defined these standard roles with the assistance of providers and state staff in other states. We can easily configure the roles based on input from providers and DHHR staff. The "Super User" role will be validated with all appropriate access during the design sessions. AuthentiCare's solution for role-based permissions is compliant with NIST guidance for identification, authentication, and authorization. Along with our robust reporting engine where reports can be scheduled regularly or run on-demand, AuthentiCare provides role-based dashboards that bring together real-time information from the EVV system database. There are many data summaries within AuthentiCare that allow EVV users to drill down to detailed data based on their role and authorized rights. One example is in our dashboards. Dashboards show real-time monitoring information to providers and administrative staff. This information is presented graphically and provides easy navigation to the source data represented in the dashboard. The Provider Dashboard shown in Figure 6.8 delivers the status of un-submitted claims and of today's scheduled visits.		

Req. ID #	Requirement Text	Requirement Type

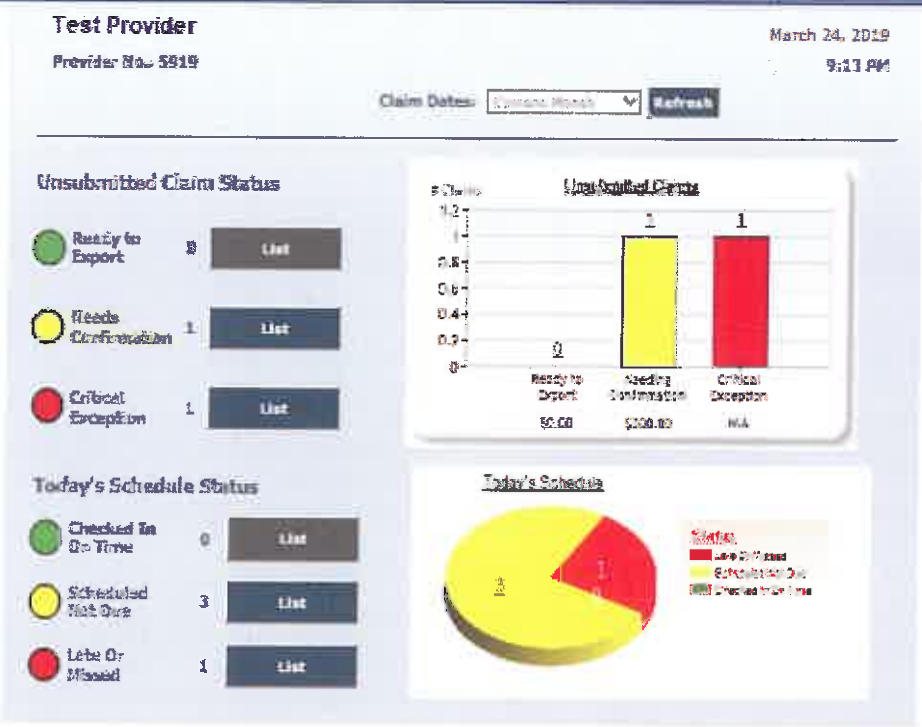


Figure 6.8 – Provider Agency Dashboard

The Worker Dashboard in Figure 6.9 shows the status of each scheduled worker. The data within each of the columns may be sorted by clicking on the column heading.

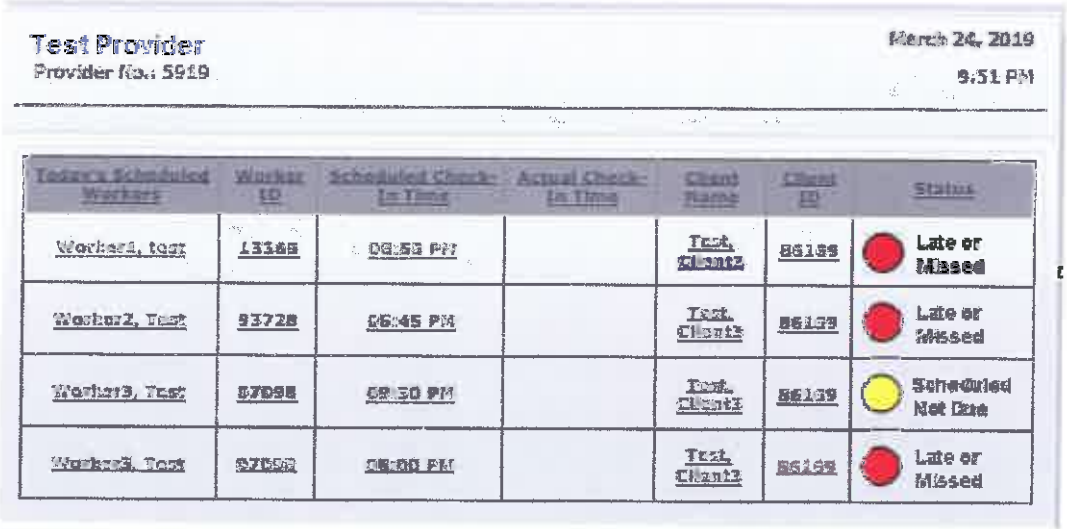


Figure 6.9 – Worker Dashboard

The Case Manager Dashboard in Figure 6.10 provides quick access to scheduled services and authorizations for customers in their assigned caseload including the authorization status.

Req. ID #	Requirement Text	Requirement Type

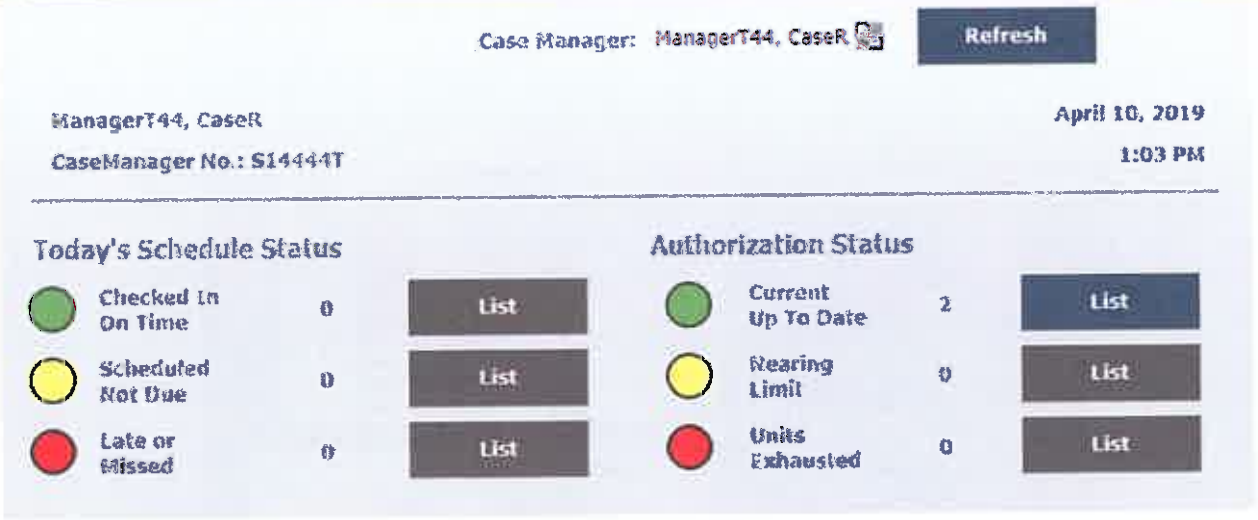


Figure 6.10 – Case Manager Dashboard

Clicking on the "List" button next to a status, like "Late or Missed" brings up a list of all the corresponding visits in the system. Users can then sort or click on individual visit records in the list to drill down, evaluate, and address issues that they find with simple, one-click access. DHHR and provider agencies can use dashboards to monitor ongoing activities and to take steps to confirm that essential services are provided, such as being able to send a back-up worker if the primary worker is delayed or absent.

With the three tools of Claims Search, Reporting Engine, and Dashboards, AuthentiCare EVV users can quickly and intuitively find and drill down into real-time activity information supporting intelligent business decisions.

PI011	The solution should track and report modifications to the solution data input elements after the direct care worker has documented their time or services, including the name of the user making the changes and the reason for the changes.	Program Integrity

The AuthentiCare visit editing page maintains a full audit trail of all data modifications to the data item level including what was changed and how it was changed, and displays a summary of who made edits and when. AuthentiCare audit reporting includes, for example, a Claim History report to show more details of edits and changes and to support viewing of claim notes added to each record.

The AuthentiCare EVV platform maintains a full audit trail of data record creation and updates. Online history reports are available for EVV visits and authorizations, while audit records for other data (Services, Clients, Providers, Caregivers, Schedules, and others) are maintained and available from FDGS. AuthentiCare maintains operational logs of system activity of each web service transaction to AuthentiCare from the mobile app per HIPAA standards. These are also used to investigate any issues the users may have had with operating the system. Audit logs cannot be modified.

7.0 Attachment 8: Technical Specifications Approach

RFP Section 5.4.2.10 (Table 11), Attachment 8, & 4.4.2, pp. 74, 119, 51
Technical specifications include those that drive how systems should be designed and built in a way that provides for long-term use and reuse, in compliance with related standards (e.g., service oriented architecture, State, and the Department of Health and Human Resources (DHHR) adopted standards, Medicaid Information Technology Architecture (MITA), and the Centers for Medicare & Medicaid Services (CMS) Conditions and Standards), as well as defining the minimum set of technical capabilities expected from certain infrastructure components.
1.1 The Vendor should provide a narrative overview of how the proposed system will meet the specifications and narrative in this request for proposal (RFP). Use the response sections to provide specific details of the proposed approach to meeting the technical specifications in each subject matter area. Responses should reference specifications and relevant mandatory requirements using the appropriate IDs from Appendix 1: Detailed Specifications and Attachment 6: Mandatory Requirements. DHHR also expects the Vendor to propose its approach for meeting any narrative in Section 4: Project Specifications in this RFP.
1.2 Responses in this section should be highly focused on DHHR business processes and specifications.
1.3 If the Vendor is proposing a phased implementation, indicate how that approach may or may not impact functionality.
1.4 Additionally, the Vendor should indicate exception handling processes where appropriate and any dependencies on existing systems or components of the new system to provide the specified functionality.
1.5 The Vendor's proposal should include one (1) or more diagrams where necessary that detail the proposed design and the relationships between key technical components.

FDGS recognizes that West Virginia is seeking an EVV system that is built in a way that provides for long-term use and reuse, in compliance with related standards.

We are responding with our Software as a Service (SaaS) solution, based on a hosted model. This approach brings a number of benefits versus an in-house, on-premise solution. These benefits:

- Provide superior security controls
- Scale cost effectively by balancing infrastructure costs across the volumes of many clients
- Are flexible and responsive in providing updates to all our clients as Medicaid rules change, thus maintaining compliance with policy updates or program changes
- Keep our solution up to date for all clients as new technologies and functions are made available
- Provide a cost-effective solution for the State

We understand that the EVV solution must also follow federal and state standards for implementation and operations, meet the Department's technical requirements, and provide a high-quality, secure environment to support an ongoing business model every day of the year. In this section, FDGS provides a focused response to address each of the subject matter areas within Attachment 8: Technical Specifications.

Solution architecture based on industry standards

In support of Medicaid Information Technology Architecture's (MITA's) Modularity Standard, AuthentiCare uses a modular, flexible approach to systems development. This includes the use of open interfaces and exposed application programming interfaces (APIs) to separate business rules from core programming. It also makes business rules available in both human and

machine-readable formats. Most business rules in AuthentiCare are captured in metadata tables in the database so they are easily edited and updated as business rules change.

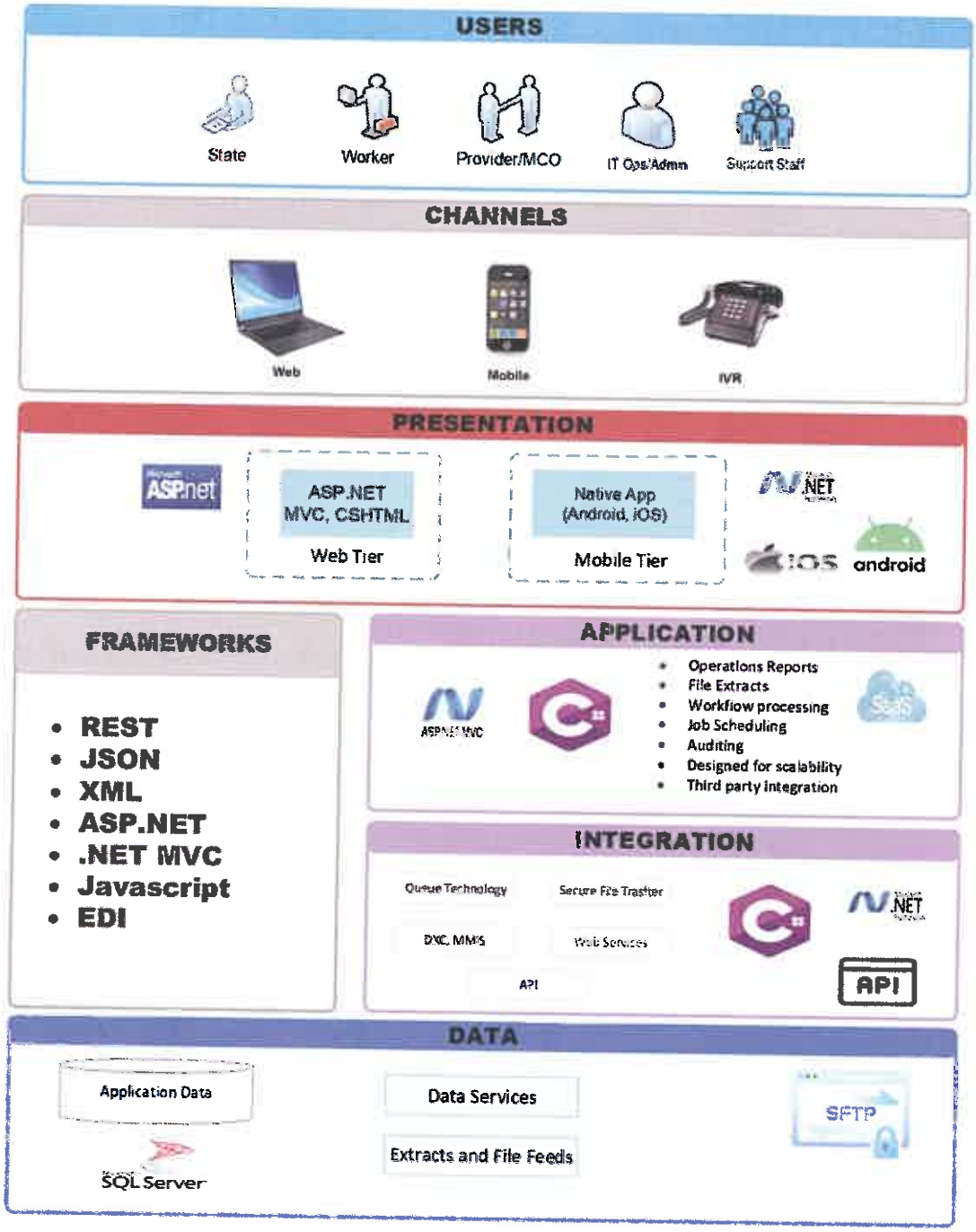


Figure 7.1 – AuthentiCare's integration is built on open architecture standards

AuthentiCare's EVV solution architecture is based on a Service Oriented Architecture (SOA) and open standards for data integration, which is beneficial for multiple system integrations. AuthentiCare web services are available for other customer-approved systems external to EVV. FDGS adopted SOA to meet our customers' current and future business requirements while maintaining security, scalability, reliability, and availability expectations. DHHR systems,

including the DXC-based MMIS, can interface with AuthentiCare through the latest industry-standard specification (JSON/REST) web service transactions or, as an alternative, the standard XML file Application Programmer Interfaces (APIs) that FDGS hosts.

AuthentiCare provides the highest level of data security and protection

Data integrity, privacy, and protection are vital components of any EVV solution for West Virginia. The EVV vendor you choose should be able to demonstrate that its provider and recipient data are scoped and meet all privacy requirements, as well as HIPAA and PHI compliance, while supporting role-based views for the State, providers, Case Managers, and Care Coordinators. Our AuthentiCare solution provides data scoping and fully complies with HIPAA and HITECH requirements.

AuthentiCare resides within Fiserv's world-class data center facilities located in Chandler, Arizona and Omaha, Nebraska, sharing the same global security policies for HIPAA and HITECH that protect our other transaction processing environments.

7.1 Data Sources, Delivery, and Display

RFP Section Attachment 8 – 2-2.1 & 4.4.2.1, pp. 119, 52
2. Data Sources, Delivery, and Display
Refer to the relevant technical specifications located in Appendix 1: Detailed Specifications and pertinent narrative in Section 4: Project Specifications in this RFP to cover solution capabilities in this area.
2.1 The Vendor should describe its approach to Data Sources, Delivery, and Display below. The narrative response for this category should be organized using the appropriate subject matter area as per Appendix 1: Detailed Specifications.

This sub-section describes our approach to data sources, delivery, and display. FDGS provides additional detail in this sub-section to meet the mandatory requirements listed in Table 7.1 as part of RFP Attachment 6: Mandatory Requirements.

Table 7.1 – AuthentiCare meets all mandatory requirements for Data Sources, Delivery, and Display

Met	Req ID #	Requirement Text
☑	**MR014**	The solution must have the ability to receive data from approved electronic visit verification (EVV) data partners and aggregate the external data into the overall solution, through the Department's approved file format and transfer method(s).

The AuthentiCare solution provides sophisticated, real-time location, time, and service data capture as recipients receive services. Our solution includes a set of modules for scheduling and appointments, time and attendance tracking, claim creation and editing, billing, and configurable reporting to meet the business rule requirements of different Medicaid-related programs and waivers. We have recently added electronic signature attestation to the AuthentiCare mobile app. Additional biometric visit verification enhancements are in design at this time.

FDGS provides additional detail to the Data Sources, Delivery, and Display Subject Matter Area requirements in Table 7.2.

Table 7.2 – Detailed Response to Data Sources, Delivery, and Display Requirements

Req. ID #	Requirement Text	Requirement Type
DD001	The Vendor should develop and provide to the Department a Logical Data Model (LDM) that includes, but is not limited to:	Data Sources, Delivery, & Display
DD002	Data classes	Data Sources, Delivery, & Display
DD003	Attributes	Data Sources, Delivery, & Display
DD004	Relationships	Data Sources, Delivery, & Display
DD005	Standards	Data Sources, Delivery, & Display
DD006	Other data elements identified by the Department	Data Sources, Delivery, & Display
We will meet this requirement with the appropriate proprietary controls in place. The Logical Data Model (LDM) and related system details are considered proprietary and confidential. If awarded, FDGS asks to review this and similar requirements that ask for proprietary AuthentiCare system details that cannot become public domain. As a SaaS offering, our policy is to protect our client's sensitive information. Allowing solution details such as our		

Req. ID #	Requirement Text	Requirement Type
Logical Data Model to become part of the public record could create vulnerabilities. Therefore, to meet requirements involving proprietary details of the AuthentiCare solution and infrastructure, we will work with the Department to establish the appropriate security controls including a Non-Disclosure Agreement (NDA), if needed.		
DD007	The Vendor should provide a complete list of data elements along with corresponding definitions for reporting purposes, upon request	Data Sources, Delivery, & Display
We will meet this requirement with the appropriate proprietary controls in place. FDGS is able to provide the details necessary to clearly document the use of our reporting components across all AuthentiCare data elements. The requested data elements, along with corresponding definitions, are considered proprietary and confidential. If awarded, FDGS asks to review this and similar requirements that ask for proprietary AuthentiCare system details that cannot become public domain. As a SaaS offering, our policy is to protect our client's sensitive information. Allowing solution details such as our data dictionaries to become part of the public record could create vulnerabilities. Therefore, to meet requirements involving proprietary details of the AuthentiCare solution and infrastructure, we will work with the Department to establish the appropriate security controls including a Non-Disclosure Agreement (NDA), if needed.		
DD008	The solution should provide real-time access to data entered into the system to provide insight for the services being provided and oversee user activity.	Data Sources, Delivery, & Display
EVV data comes into AuthentiCare in real time from the Mobile App, IVR, and Web. Report data are also shown in real time, and include all relevant EVV data right up to the time the requested report runs. Small provider offices frequently run the Time and Attendance Report for the current day throughout the day to view service visits as they occur to confirm service provision to clients. Knowing the location of workers also assists in notification of workers for client updates and schedule changes.		
DD009	The solution should employ online real-time or batch updates of data between the solution and other systems including, but are not limited to, the Medicaid Management Information System (MMIS) and other third-party Electronic Visit Verification (EVV) systems.	Data Sources, Delivery, & Display

As an experienced and mature EVV solution, AuthentiCare is capable of integrating data as part of our successful EVV solution, including the transfer of data to and from other systems on a schedule that FDGS and the Department agree on. The two most common file transfers or interfaces are batch processing (usually daily, but can be executed on a different schedule) and web service exchange (real time).

For batch processing, AuthentiCare receives data from provider agencies, support coordinators, the State's fiscal agent, or other external stakeholders daily and processes during a defined timeframe. AuthentiCare receives these imports in an XML format and then imports them into AuthentiCare's databases. Once a file is imported, an import results file is created that shows the success or failure of the overall process and lists any error records with the reason for the error. Bulk file exchanges with the state or with MCO trading partners use our File Gateway to transfer files by SFTP. Providers drop off and pick up smaller files using a secure web portal. Providers can receive email notification when their files have processed and results are ready to pick up.

For web service interaction, the same data elements are transmitted in real time, using secure web services APIs. AuthentiCare uses an industry standard JavaScript Object Notation/Representational State Transfer (JSON/REST) format. Having data updated in real time improves accuracy and timely reporting, including interactive dashboard updates.

Table 7.3 identifies the standard data transfers that are often required when implementing and updating an EVV solution.

Table 7.3 – Standard Data Updates to and from AuthentiCare

Name	Usual Source	Description
Authorization Import	The State or MCOs	Load New/Changed Authorizations from an external system (provider agency, support coordinator, fiscal agent, MMIS system, or other state database) to AuthentiCare. This can include the plan of care tasks to be completed. Once a visit is verified, the tasks provided by the attendant can be compared to the plan of care.
Beneficiary Import	The State or MCOs	Load New/Changed Beneficiary (service recipient) enrollment details from an external system (provider agency, support coordinator, fiscal agent, MMIS system, or other state database) to AuthentiCare.

Req. ID #	Requirement Text		Requirement Type
Provider Import	The State or MCOs	Load New/Changed Provider enrollment details from an external system (provider agency, support coordinator, fiscal agent, MMIS system, other state database) to AuthentiCare.	
Case Manager Import	The State or MCOs	Load New/Changed Case Managers/Care Coordinators data from an external system (provider agency, support coordinator, fiscal agent, MMIS system, or other state database) to AuthentiCare.	
837P, 837I Claim Export	AuthentiCare to the State or MCOs	Submit authorized and confirmed claims for EVV services to MCO payers or the state MMIS on behalf of Providers.	
835 Payment Files	Providers	Receive 835 payment files from providers, and report on claim payments and denials.	
Worker Schedules	Providers	For Providers that have their own scheduling system, FDGS can accept file uploads of worker schedules to input or update schedules in AuthentiCare.	
Worker Import	Providers	Providers manage their workers directly through the administrative portal. If a provider requires a complete import of worker data, FDGS can work with them on data elements and formats to submit a full worker upload.	
DD010	The solution should have the ability to integrate client data for all programs served by the solution into the Master Data Management (MDM) platform.		Data Sources, Delivery, & Display
FDGS will provide the interface specification and develop the data extract of the client data for integration into the MDM platform. Per Addendum 6, DHHR response to Q065, FDGS understands that AuthentiCare will primarily interface with the MMIS system which is similar to our integration for several other AuthentiCare statewide clients.			
DD011	The solution should allow users to extract data, manipulate the extracted data, and specify the desired format of the output.		Data Sources, Delivery, & Display
AuthentiCare report data are available in Excel, CSV, and XML and can be extracted by state staff, MCOs, providers, and other authorized users to merge with existing data for additional manipulation, and report design and generation. The main reports engine web page provides easy access to run on-demand reports, create and schedule regular reports for re-use, and then pick up completed reports in the user's preferred format (including PDF, Excel, and XML). The system allows the user to schedule or submit report requests, do other work while the reports run, and come back to the page to pick up the reports when they are ready.			
DD012	The solution should provide required Federal and Department data sharing including high-speed data transfer functionality to send and receive information.		Data Sources, Delivery, & Display
The AuthentiCare solution will use our industry-standard APIs and web services to connect with existing workflow, ESB orchestration components, and other authorized systems for event-driven processes and required Federal and Department data sharing. Data transfer rates for send and receive will meet approved service levels. AuthentiCare's integration capabilities are based entirely on open-systems standards and accommodate communications to database management systems and back-end solutions through APIs and custom imports and exports. Additional features, such as EDI 837 file creation, are built into the AuthentiCare solution and leverage the open standard architecture. AuthentiCare's feature-rich solution supports MITA's seven conditions and standards to provide required high-speed data transfer functionality to send and receive information. FDGS will collaborate with DHHR to determine the required source systems, data files, required data elements, file transfer protocols, and file interface definitions to successfully operate AuthentiCare as noted in Addendum 6, Q066.			
DD013	The solutions rules/procedures should allow for electronic communication between the Department, fiscal/employer agents, and providers.		Data Sources, Delivery, & Display
The AuthentiCare solution does not currently support electronic communication between end users. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.			
DD014	The solution should have the ability to store member communications.		Data Sources, Delivery, & Display
The AuthentiCare solution does not currently support electronic communication between end users. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding			

Req. ID #	Requirement Text	Requirement Type
quoted in the cost response once Phase 1 has been successfully implemented.		
DD015	The solution should exchange information through interfaces including, but not limited to the Medicaid Management Information System (MMIS), other Electronic Visit Verification (EVV) systems, and others as agreed upon by the Department.	Data Sources, Delivery, & Display

Similar to DD012, the AuthentiCare EVV solution will use our industry-standard APIs and web services to connect with existing workflow, ESB orchestration components, and other authorized systems—including other EVV systems—for event-driven processes and data sharing where appropriate.

AuthentiCare's Data Aggregator can be configured to import data from other EVV systems so that the Department has a common repository of all EVV data collected. The AuthentiCare solution provides for an EVV interface with existing third-party EVV systems that have been approved by DHHR to send data to the AuthentiCare solution for unified statewide reporting. Using our web services provides near real-time processing of data collected through AuthentiCare's Data Aggregator.

DD016	The solution should have the ability to interface with West Virginia's Enterprise Service Bus (ESB).	Data Sources, Delivery, & Display

FDGS has significant experience integrating AuthentiCare into client systems to support data transfers necessary for EVV functionality. We will work with the Department to establish appropriate connectivity through our APIs to the West Virginia ESB. The hosted AuthentiCare EVV solution will use our industry-standard APIs and web services to connect with existing workflow and ESB orchestration components for event-driven processes and data sharing where appropriate.

AuthentiCare's service endpoints, APIs, and web services will be exposed to the ESB for both inbound and outbound messages. Our EVV solution architecture is based on a Service Oriented Architecture (SOA), which is beneficial for multiple system integrations. AuthentiCare web services are available for other customer-approved systems external to EVV. FDGS adopted SOA to meet our customers' current and future business requirements while maintaining security, scalability, reliability, and availability expectations.

Agency systems, including the State MMIS, can interface with AuthentiCare through the latest industry-standard specification (JSON/REST) web service transactions or, as an alternative, the standard XML file Application Programmer Interfaces (APIs) hosted by Fiserv. Currently, AuthentiCare has successfully managed file API integrations with MMIS in production in five states (South Carolina, Kansas, Oklahoma, Nevada, and Alabama) plus the U.S. Veterans Health Administration. This API infrastructure has proven successful in production operations since its launch in 2013.

DD017	The Vendor should complete, subject to approval by the Department, the interface with the Medicaid Management Information System (MMIS).	Data Sources, Delivery, & Display

Our AuthentiCare team has worked with your MMIS vendor, DXC, in multiple states. FDGS staff are experienced in working with different state agencies with multiple vendors. For example, for the Nevada AuthentiCare implementation, coordination with DXC for interfaces was essential to receiving provider and member data, and our staff was able to work with all MCOs to facilitate authorizations and 837/835 integration.

FDGS will coordinate and cooperate, as directed by DHHR, with your MMIS vendor to formalize and finalize the required configuration for interfaces. We have successfully built and continue to maintain interfaces to DXC-managed—and other state—MMIS systems. Further, we have a successful record of submitting claims at a high rate of accuracy. As part of our integration into MMIS systems from various states, 99.4 percent of first-pass claims submitted from AuthentiCare to their system paid successfully, resulting in less post-adjudication adjustments and rework. We anticipate having the same type of success integrating into the West Virginia MMIS and related systems for provider claims submissions and similar data exchanges.

Currently, AuthentiCare is integrated with DXC-operated and managed MMIS systems in:

- Oklahoma (DXC/interChange): Since beginning our operation in 2009, AuthentiCare has processed 4 million claims annually for more than 300 provider locations and 26,000 beneficiaries. 99.5 percent of submitted claims were transmitted and paid via an 837 specification compliant file to the DXC MMIS portal.
- Kansas (DXC/interChange): Since 2010, AuthentiCare has processed 4 million claims annually for more than 600 provider locations and 21,000 beneficiaries. 99.3 percent of submitted claims were transmitted via an 837 specification compliant file to the DXC MMIS portal for adjudication.
- Alabama (DXC/interChange): AuthentiCare went live on October 1, 2017. Since then, over 5 million claims have been processed, and 837 and 835 files are being exchanged via secure File Gateway with the DXC-operated and

Req. ID #	Requirement Text	Requirement Type
	managed MMIS system. 98.9 percent of claims submitted to the DXC MMIS portal were successfully paid.	
DD018	The solution should be able to receive information in batch and in individual transactions on a schedule agreed upon by the Department.	Data Sources, Delivery, & Display
	AuthentiCare supports data capture via individual transactions as well as batch processes run on an agreed upon schedule. As an experienced EVV provider, FDGS is skilled in integrating all components of a successful EVV solution, including the automatic loading of beneficiary, provider, and plan of care (authorization including individual tasks) data. The two most common interfaces are batch processing (daily) and web service exchange (real time). For batch processing, AuthentiCare receives data from provider agencies, support coordinators, the State's fiscal agent, or other external stakeholders daily and processes during a defined timeframe. AuthentiCare receives these imports in an XML format and then imports them into AuthentiCare's databases. Once a file is imported, an import results file is created that shows the success or failure of the overall process and lists any error records with the reason for the error. Bulk file exchanges with the State or with MCO trading partners use our File Gateway to transfer files by SFTP. Providers drop off and pick up smaller files using a secure web portal. Providers can receive email notification when their files have processed and results are ready to pick up. AuthentiCare's real-time interfaces, or web services, return success or failure to the sender as part of the API. An error listing is provided in our documentation to identify the failure so the sender can identify the resolution. Batch processing supports notification for failed file transfers as well as results files indicating details of success or failure. Anonymous actions, like workflows and backend processing, create logging and alerts for operational review. For all failed processes, recovery procedures are performed by AuthentiCare operations and support staff. The Operations team is notified of failures for resolution or escalation, if required.	
DD019	The solution should have the ability to receive provider, member, and prior authorization data from the Medicaid Management Information System (MMIS) at a frequency and format determined by the Department.	Data Sources, Delivery, & Display
	AuthentiCare is able to receive updates to provider, member, and prior authorization data as supplied by the MMIS. We support both real-time updates via API and daily batch files. FDGS will work with the Department to identify the appropriate interface, format, and timing. Our hosted SaaS platform provides a standard XML file API and standard JSON/REST web service API for prior authorizations. These APIs can be configured to meet the MMIS integration requirements. Use of proven, standard APIs provides a smooth, low-risk startup of EVV and transition from legacy MMIS, while maintaining full operations and client care. Support is provided for other standard interfaces including X12 278 Request and Response, and initial bulk data upload.	
DD020	The solution's data aggregation component should be able to receive a response transaction in a format that is used by the Medicaid Management Information System (MMIS) for the purpose of verifying edits to claims.	Data Sources, Delivery, & Display
	AuthentiCare's Data Aggregator can be configured to import data so that the Department has a common repository of all EVV data collected in a format that is consumable by the MMIS for the purpose of verifying edits to claims. The AuthentiCare solution provides for an EVV interface with existing third-party EVV systems that have been approved by DHHR to send data to the AuthentiCare solution for unified statewide reporting. Using our web services provides near real-time processing of data collected through our Data Aggregator. EVV required data, including visit data from GPS and other alternative location methods, are accepted if provided by external systems and retain an identifier to note from which system the data were captured. As data are aggregated into AuthentiCare, provider reports for verified visits by the billing provider, visits that were not verified, and others are available. To maintain secure access to report data, provider agencies must securely log in to access their respective Reports page to review their reports. AuthentiCare allows reports to be downloaded to PDF, Excel, and CSV formats. AuthentiCare supports the calculation of total daily and weekly hours worked by the direct care worker and aggregate hours across payers, programs, providers, and recipients receiving services through the master worker function. This collects the hours as some direct care worker may support different providers. These data are compiled through multiple sources. In order to aggregate across providers and payers, each direct care worker will require a unique ID when registered by the provider. Our Data Aggregator solution provides the MCOs and providers different options and capabilities to move data automatically in and out of AuthentiCare so that they can choose the transport method and format most compatible with their existing systems. The process can accept data through three different channels: • Web service upload (real-time communications): Users can upload claim or encounter records for visits in batches	

Req. ID #	Requirement Text	Requirement Type
	of up to 500 records per transaction through a secure JSON/REST web service portal. Not all provider EVV systems support real-time data exchange, but AuthentiCare does. • Web portal upload: For smaller providers, claim or encounter files can be uploaded through a secure web portal. When the file import finishes, the user can download an import results file that lists any error messages or rejected records. • SFTP file gateway upload: For large providers or EVV service bureaus that produce large files, AuthentiCare can accept files through a secure SFTP gateway portal. Import results can be posted back to the same portal for subsequent pickup. Claim and encounter processing into AuthentiCare is queued such that the Aggregator can be highly available. During maintenance, import processing continues onto the queues so that users can receive their import results quickly. When maintenance is completed, the data are automatically processed and users will have experienced only a slight delay in their data appearing on the AuthentiCare web and in reports.	
DD021	The solution should have the ability to apply pre-edit information and serve as a data source for purposes of applying edits during claims processing. The disposition of the edit including, but not limited to deny or suspend, should be determined by the Medicaid Management Information System (MMIS).	Data Sources, Delivery, & Display
	AuthentiCare is able to apply pre-edits through the "claim scrub" process and then submit new claims to the MMIS as long as they pass the pre-edits without exception. If AuthentiCare is later provided an MMIS denial in the 835, it is then able to submit replacement claims. Provider adjustments or voids to allow submission of replacement claims must be determined from within the MMIS and completed there where all of the business rules and user edits are available.	
DD022	The solution should accept individual and/or batch visit verification inquiries from the Medicaid Management Information System (MMIS).	Data Sources, Delivery, & Display
DD023	Member name	Data Sources, Delivery, & Display
DD024	Billing provider	Data Sources, Delivery, & Display
DD025	Name	Data Sources, Delivery, & Display
DD026	Date	Data Sources, Delivery, & Display
DD027	Time of service delivery	Data Sources, Delivery, & Display
	AuthentiCare supports both individual and batch inquiries from external systems including the MMIS. We support both real-time updates via API and daily/scheduled batch files. Information provided includes member name, billing provider, name, date and time of service delivery.	
DD028	The solution should have the ability to provide visit information to the Medicaid Management Information System (MMIS) by individual and/or in batch format at the discretion of the Department.	Data Sources, Delivery, & Display
	AuthentiCare incorporates an ANSI X12 standard EDI process for billing confirmed claims. This process automatically routes the claims to the MMIS. AuthentiCare creates and submits both 837P and 837I for states today. FDGS will coordinate and cooperate, as directed by the Department, with its MMIS vendor to formalize and finalize the required configuration for interfacing visit information for individual or batch format. We have successfully built, and continue to maintain, interfaces to DXC-managed—and other state—MMIS systems. Further, we have a successful record of submitting claims at a high rate of accuracy. As part of our integration into MMIS systems from various states, 99.4 percent of first-pass claims submitted from AuthentiCare to their system paid successfully, resulting in less post-adjudication adjustments and rework. We anticipate having the same type of success integrating into the West Virginia MMIS and related systems for provider claims submissions and similar data exchanges.	
DD029	The solution should support obtaining member eligibility information through the current Medicaid Management Information System (MMIS) solution using industry standard data interfaces and exchanges as defined by X12N 270/271 transactions. (Reference: http://www.wpc-edi.com/)	Data Sources, Delivery, & Display
	AuthentiCare web services support 270 Eligibility Request and 271 Eligibility Response. We will work with DHHR to interface with its MMIS to accept timely data updates to Member Eligibility Data when modified. Our experience has been that some manual entry has been required to accommodate missing data provided in the eligibility process.	

Req. ID #	Requirement Text	Requirement Type
DD030	The solution should conform to ASC X12 Technical Reports Type 3 (TR3), Version 005010. (Reference http://www.wpc-edi.com/)	Data Sources, Delivery, & Display
AuthentiCare incorporates the ANSI X12 TR3 standard EDI process for billing confirmed claims. This process automatically routes the claims to the MMIS. FDGS creates and submits both 837P and 837I for states today in compliance with this standard. The AuthentiCare SaaS platform provides a standard XML file API and standard JSON/REST web service API for service authorizations. These APIs can be configured to meet Department standards. Use of proven, standard APIs provides a smooth, low-risk startup of EVV, integration with the legacy MMIS, while maintaining full operations and client care. Support is provided for X12 278 Request and Response, as well as initial bulk data upload.		
DD031	The solution should generate all forms and notices as necessary.	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD032	The solution should have the ability to schedule alerts and user notifications.	Data Sources, Delivery, & Display
AuthentiCare delivers the ability to configure automated alerts, such as when services are late or missed, so a qualified back-up worker may be dispatched. Automated alerts may be sent via email to designated recipients as determined by Department policy. Support coordinators, provider agencies, emergency back-up workers, or state staff may be notified that a critical service has not been delivered. Alerts may also be configured to meet the requirements of individual services or programs as chosen by the Department, and alerts can go to multiple recipients as defined in the template. These alerts can be tracked by caregiver, provider, or recipient in various reports and dashboards to identify trends that need to be addressed. To prevent "alert fatigue," it is critical to define timing and escalation of the alerts to maximize the meaning of an alert when it is received, and minimize the number of false alarms. AuthentiCare alert thresholds can use statewide default values or specific values for a type of service. Optionally, there can be special values for specific critical recipient needs, like for at-risk recipients. Alerts can be disabled for some services (for example, services that are not scheduled, or unit-based services like Home Delivered Meals), or for situations where the recipient is in a remote "no tech zone" where the visit data will be submitted by Store and Forward from the Mobile App at a later time. These options reduce false alarms. Automated alerts are sent via email to designated recipients. Support coordinators, provider agencies, emergency back-up workers, or State staff may be registered to be notified that a critical service has not been delivered. For example, AuthentiCare can be configured so that only Providers receive late alerts whereas care managers, State staff, or others could be notified of missed alerts only. AuthentiCare is easily configurable to set up multi-level escalating alerts for late or missed visits as needed by the Department.		
DD033	The solution should allow printing of blank and completed documents including, but not limited to:	Data Sources, Delivery, & Display
DD034	All forms	Data Sources, Delivery, & Display
DD035	All system-generated correspondence	Data Sources, Delivery, & Display
DD036	Reports	Data Sources, Delivery, & Display
All reports are printable from the browser or as PDF documents. AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD037	The solution should generate and supply forms in the following methods, including, but not limited to:	Data Sources, Delivery, & Display
DD038	Email	Data Sources, Delivery, & Display

Req. ID #	Requirement Text	Requirement Type
DD039	Download from Portal	Data Sources, Delivery, & Display
DD040	Postal Mail, upon request by the Department	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD041	The solution should allow the ability to modify field attributes on a form as identified by the Department via the Change Management Plan.	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD042	The solution should allow updates to form templates as directed by the Change Management Plan.	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD043	The solution should group related correspondence to ensure materials are delivered in a single mailing or posted to a portal account.	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD044	The solution should generate the data file containing forms and notices for delivery to the printing vendor for monthly distribution and as requested by the Department.	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD045	The solution should automatically populate information on notices or forms being issued.	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD046	The solution should generate batch forms.	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD047	The solution should save delivered forms to the user's account.	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD048	The solution should deliver data files containing all correspondence to the designated printing entity within 24 hours of the correspondence becoming final according to the Department's business rules.	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding		

Req. ID #	Requirement Text	Requirement Type
quoted in the cost response once Phase 1 has been successfully implemented.		
DD049	The solution should post finalized correspondence to the web portal, according to the Department's business rules.	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD050	The solution should have the ability to produce all correspondence in a printer-friendly 8.5" x 11" format in landscape or portrait orientation.	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD051	The solution should have the ability to automatically save a Portable Document Format (PDF) copy of each final correspondence.	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD052	The solution should allow users to choose their preferred method of correspondence including, but not limited to, email, post mail, text, or phone.	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD053	The solution should generate correspondences using pre-defined templates.	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD054	The solution should include automatic system-generated correspondence with output capabilities including, but not limited to:	Data Sources, Delivery, & Display
DD055	Email	Data Sources, Delivery, & Display
DD056	Post to user portal account	Data Sources, Delivery, & Display
DD057	Queue for printing	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD058	The solution should be able to schedule distribution of correspondence.	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD059	The solution should provide flexible web-based reporting that meets external reporting needs and requirements defined by the Department.	Data Sources, Delivery, & Display
The main reports engine web page provides easy access to run on-demand reports, as well as create and schedule regular reports for re-use, and then pick up completed reports in the user's preferred format (including PDF, Excel, and XML). AuthentiCare offers a series of standard reports as shown in Table 6.6 below. Users may also define various filters to tailor the output for specific reporting needs. The system allows the user to schedule or submit report requests,		

Req. ID #	Requirement Text	Requirement Type
do other work while the reports run, and then come back to the page to pick up the reports when they are ready.		
DD060	The solution should include a standard library of reports that can be generated by any user with appropriate access.	Data Sources, Delivery, & Display

Along with the capabilities described in DD059, AuthentiCare provides a library of standard reports that can be generated by users with the appropriate access (listed in Table 7.4 – AuthentiCare Standard Reports). Over time, as multiple customer requests are addressed for new reports, FDGS evaluates whether to add the new report to the core application and expand the library of available reports.

Table 7.4 – AuthentiCare Standard Reports

Report Name	Report Description
Authorizations	**Lists all authorization details**
Authorization History	Gives authorization history and highlights new or changed authorizations
Authorizations w/ Claim Details	Lists authorization details and associated claims information. Therefore, this report gives the user authorization utilization information
Billing Invoice	Lists claims by service date and export/submission date, along with the billing status and amount
Calendar	Lists all scheduled events
Claim Data Listing	Lists, by provider and worker, all services performed during a given time period and the total dollars billed to and paid by MMIS
Claim Details	Claim listing with details that can be grouped by beneficiary
Claim History	Reports all claim activities by referencing claim audit data
Eligible Client Data Listing	Lists the beneficiaries a provider is eligible to serve and information on each beneficiary like address, phone number, and Medicaid ID
Exception	Lists claim exceptions, as defined in the AuthentiCare workflow
Late and Missed Visits	Details late and missed visits and any selected reason codes
Overlapped Claim By Client	Identifies beneficiaries that have two workers providing care at the same time
Overlapped Claim By Worker	Identifies workers who are servicing two beneficiaries at the same time
Provider Activity	Lists services performed during a given time period and the total dollars billed to MMIS (or MCO), by worker
Remittance Advice	Details remittance advice status, allowing providers to examine paid claims, and reconcile payment amounts
Remittance Data Listing	Lists, by provider, all remittance records (payments and denials) so that the provider can examine paid claims and reconcile payments
Time and Attendance	Reports check-in and check-out times
Unauthorized Location	Highlights mobile app visits recorded from an unauthorized GPS location
Unauthorized Phone Number	Highlights IVR calls made from an unauthorized phone
Worker Activity	Displays check-in/out times only and no billing information. Also displays any claim notes

Req. ID #	Requirement Text	Requirement Type
DD061	The solution should have the ability to display the number of pages that should be printed before the user proceeds with printing a report.	Data Sources, Delivery, & Display
AuthentiCare reports show "Page X of Y" on each output page. The user can decide which pages to print within the "Print..." dialog box from their browser. If exported to PDF, the software indicates the number of pages, and the user is allowed to indicate the pages or page range to print.		
DD062	The solution should have the ability to export reports directly from the solution into the user-specified format including, but not limited to:	Data Sources, Delivery, & Display
DD063	Excel	Data Sources, Delivery, & Display
DD064	Word	Data Sources, Delivery, & Display
DD065	Hyper Text Markup Language (HTML)	Data Sources, Delivery, & Display
DD066	Comma-Separated Value (CSV)	Data Sources, Delivery, & Display
DD067	Portable Document Format (PDF)	Data Sources, Delivery, & Display
AuthentiCare will support the ability to export reports into Excel, CSV, and PDF. We have found that these formats support the data export needs of our customers. Enhancements to AuthentiCare supporting exports into Word or HTML formats will be discussed with the Department with the use of the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DD068	The solution should provide reporting functionality capable of drilling down from summarized data to detailed data as agreed upon by the Department.	Data Sources, Delivery, & Display
In addition to the features described in DD059 and DD060, AuthentiCare's robust reporting engine provides a tool for easily customized EVV program monitoring and management, which helps identify and reduce fraud, waste, and abuse. AuthentiCare contains a broad spectrum of on-demand reports with ad hoc functions like drop-down list filters, parameters, date ranges, and other selections that allow users to report the data of which they are specifically interested. This allows the Department and providers the ability to search through summary and detailed data views. Using selection criteria for each report, a user can customize the standard report to meet specific requirements easily and simply, and run a one-time report, or save a report that they want to run regularly for ongoing analysis or metrics submissions. These reports provide DHHR stakeholders, as well as the provider community (based on their security access authority), views into the electronic visit and verification data to manage the programs, confirm beneficiaries receive needed care, and help identify fraud, waste, and abuse. In combination with the Reporting Engine, AuthentiCare provides a series of role-specific dashboards. There are many data summaries within AuthentiCare that allow AuthentiCare users to drill down to detailed data. One example is in our dashboards. Dashboards show real-time monitoring information to providers and administrative staff. This information is presented graphically and provides easy navigation to the source data represented in the dashboard. The Provider Dashboard shown in Figure 7.2 delivers the status of un-submitted claims and of today's scheduled visits.		

Req. ID #	Requirement Text	Requirement Type

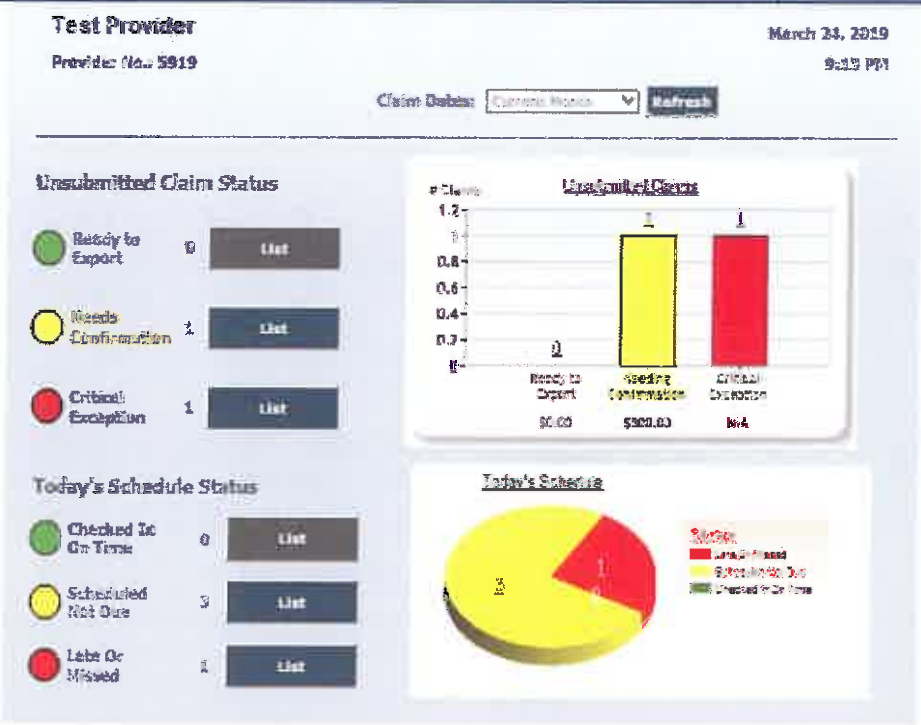


Figure 7.2 – Provider Agency Dashboard

The Worker Dashboard in Figure 6.9Figure 7.3 shows the status of each scheduled worker. Users can sort the data within each of the columns by clicking on the column heading.

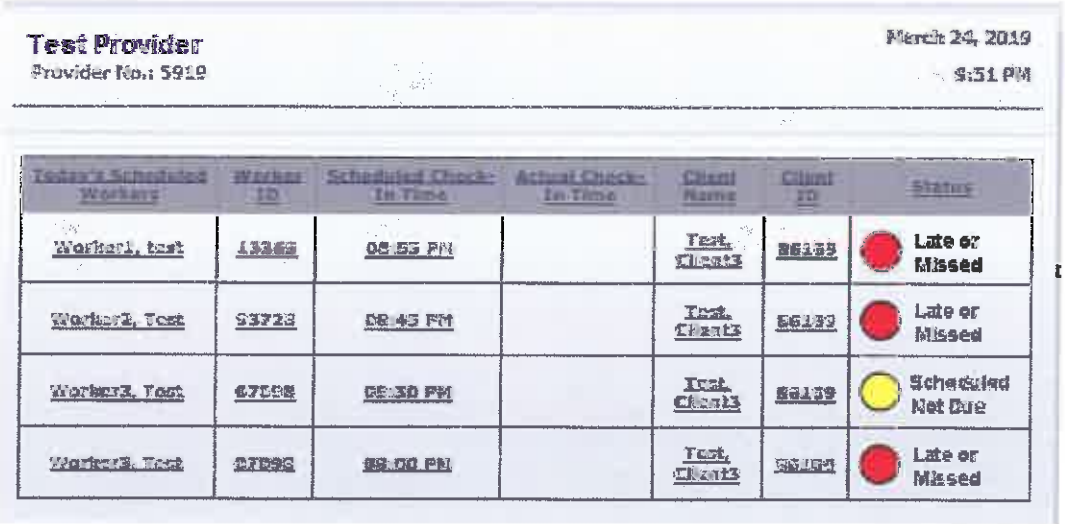


Figure 7.3 – Worker Dashboard

The Case Manager Dashboard in Figure 7.4 Figure 6.10provides quick access to scheduled services and authorizations for customers in their assigned caseload including the authorization status.

Req. ID #	Requirement Text	Requirement Type

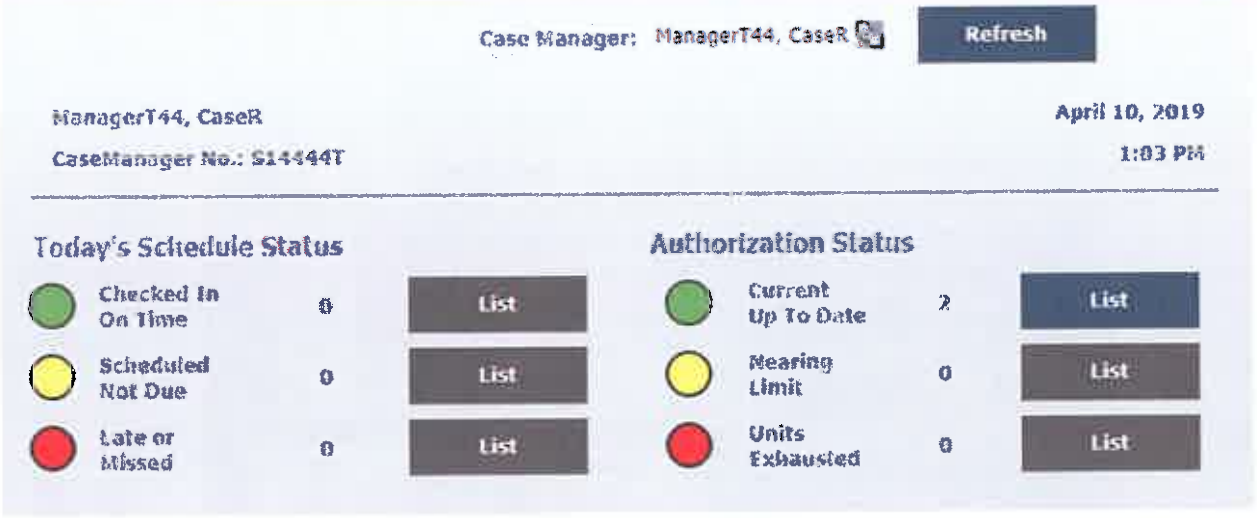


Figure 7.4 – Case Manager Dashboard

Clicking on the "List" button next to a status such as "Late or Missed" brings up a list of all the corresponding visits in the system. Users can then sort or click on individual visit records in the list to drill down, evaluate, and address issues that they find with simple, one-click access. Department and provider agencies can use dashboards to monitor ongoing activities and to take steps to confirm that essential services are provided, like being able to send a back-up worker if the primary worker is delayed or absent.

With the three tools of Claims Search, Reporting Engine, and Dashboards, AuthentiCare EVV users can quickly and intuitively find and drill down into real-time activity information supporting intelligent business decisions.

DD069	The solution should have an integrated web portal designed to interface, receive, send, and download specified content and reporting information directly from/to entities such as provider agencies, EVV Vendors, contractors, and other state and Federal agencies as part of a fully integrated solution.	Data Sources, Delivery, & Display

The AuthentiCare solution can be integrated into a larger SOA architecture using data interfaces and application programming interfaces (APIs) and can be accessed by any Medicaid enterprise application in need of our services. AuthentiCare solution processes employ data interchange and web service standards including secure JSON API and restful (REST) web services. This API infrastructure has been proven successful in production operations since launching in 2013.

AuthentiCare provides MCOs and providers different options and capabilities to move data automatically in and out of AuthentiCare so that they can choose the transport method and format most compatible with their existing systems. This reduces the time to integrate and reduces the burden on these organizations to implement. The system can accept data through three different channels:

- Web service upload (real-time communications): Users can upload claim or encounter records for visits in batches of up to 500 records per transaction through a secure JSON/REST web service portal. Not all provider EVV systems support real-time data exchange, but AuthentiCare does.
- Web portal upload: For smaller providers, claim or encounter files can be uploaded through a secure web portal. When the file import finishes, the user can download an import results file that lists any error messages or rejected records.
- SFTP file gateway upload: For large providers or EVV service bureaus that produce large files, AuthentiCare can accept files through a secure SFTP gateway portal. Import results can be posted back to the same portal for subsequent pickup.

DD070	The solution should contain the following features and capabilities including, but not limited to:	Data Sources, Delivery, & Display
DD071	Drill down and look up functionality to minimize re-entry of information across multiple screens	Data Sources, Delivery, & Display

Req. ID #	Requirement Text	Requirement Type
DD072	Multi-tasking and multiple window capability, including split screens	Data Sources, Delivery, & Display

To minimize re-entry of information across multiple windows, AuthentiCare provides automatic lookup and auto population of some fields. To maintain data integrity, fields that allow a limited list of valid values use drop-down structures so that users can only select valid entries.

AuthentiCare's intuitive user interface, navigation, and built-in workflow in both the mobile and web applications eliminates the need for splitting screens. In many instances, content included in the current window affects the navigation and relevant detail on the next page or window. However, for multi-tasking, web users may use multiple tabs in their browser to work in different areas of AuthentiCare or to manage multiple updates as often occurs throughout their work day.

Figure 7.5 shows the user hovering over the Claim ID to see the claim details popup. There is no need to re-enter IDs or other data that may be error prone due to simple typos.

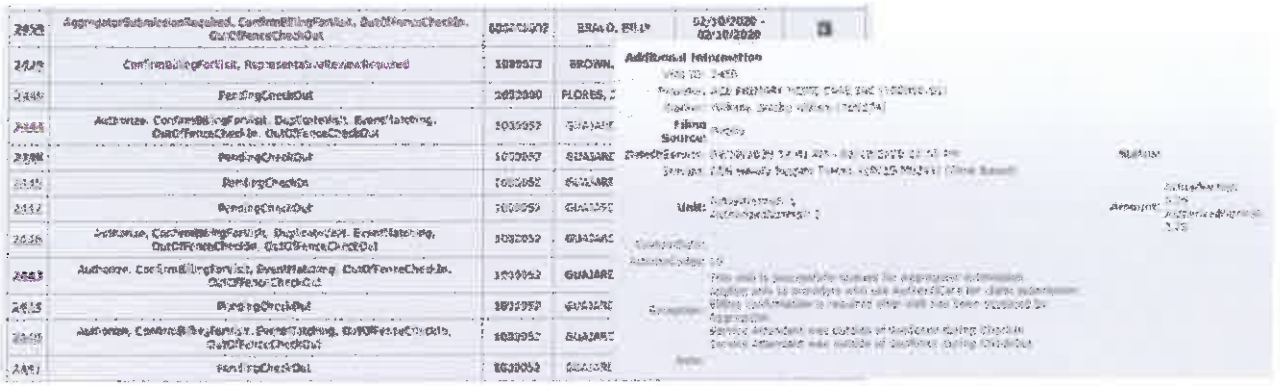


Figure 7.5 -- AuthentiCare shows details without additional data entry

Additionally, by simply clicking on the Claim ID in the results list, the user is presented the Visit Details page as displayed in Figure 7.6 – again, with no additional data entry required.

Req. ID #	Requirement Text	Requirement Type

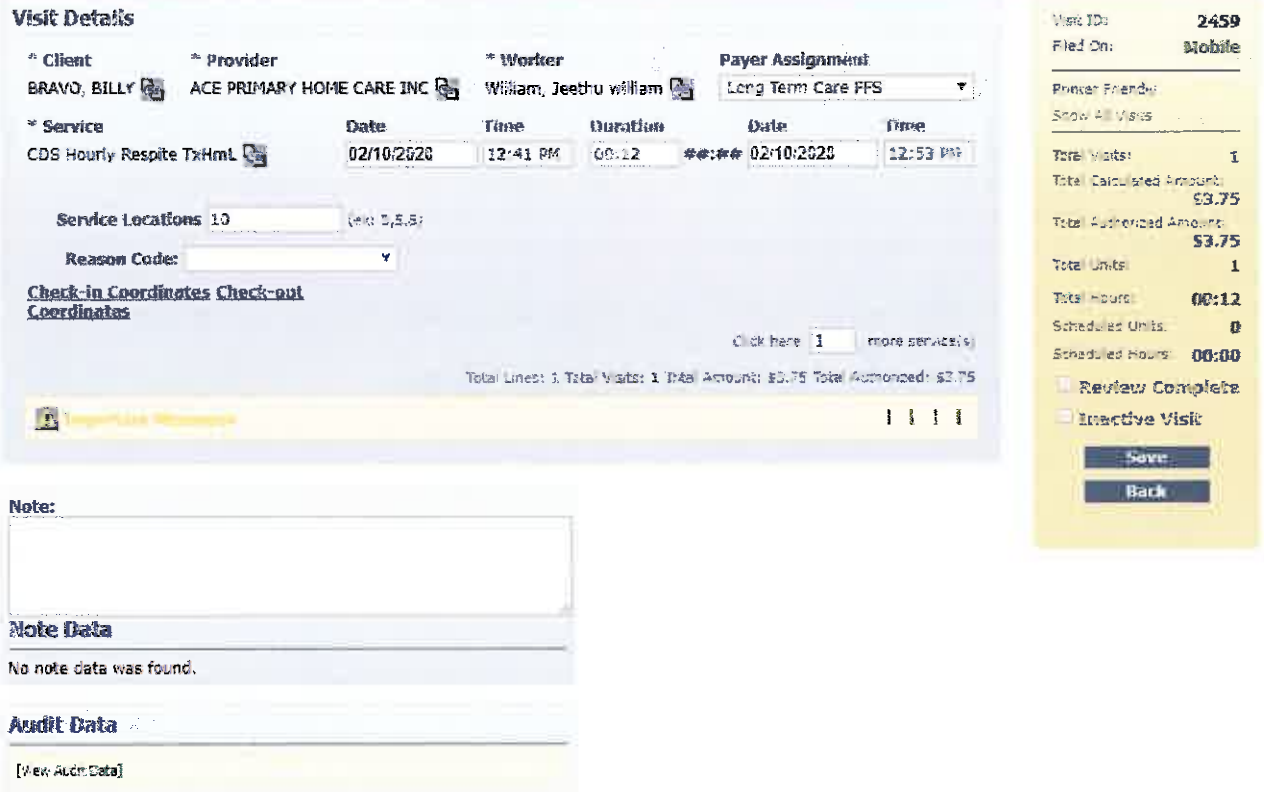


Figure 7.6 – Details are only a click away with AuthentiCare's user-friendly navigation

DD073	The solution should provide context-sensitive help to users on all screens.	Data Sources, Delivery, & Display
The AuthentiCare application offers online training and related content accessible through the application. AuthentiCare also provides worker handouts for using both the mobile and IVR methods to check-in for an EVV visit. These are available within AuthentiCare and as a PDF that can be laminated, printed, or emailed to workers. FAQs are compiled and linked from within the portal.		
DD074	The solution should provide menus that are understandable by non-technical users and provide secure access to all functional areas.	Data Sources, Delivery, & Display
The AuthentiCare solution includes intuitive, user-friendly screens in both the website and mobile application. Each screen provides easy-to-navigate menus and drop-down selections along with standard data entry that makes AuthentiCare easy to use for specialists and non-technical users alike. AuthentiCare's role-based security supports a hierarchical structure in which users are granted access to specific areas, functions, and data within the product. Users are assigned to roles that are granted specific access rights within the system. Through the AuthentiCare website and mobile application, only authorized users can create, view, and modify visits, claims, schedules, etc.		
DD075	The solution should provide a user interface that allows users to move easily throughout the system.	Data Sources, Delivery, & Display
AuthentiCare has been developed and enhanced with a simple user interface that navigates through the workflow and screens to properly manage schedules, visits, claims, and exceptions. We will share the full user interface for both the web and mobile applications during our oral presentation.		

Req. ID #	Requirement Text	Requirement Type

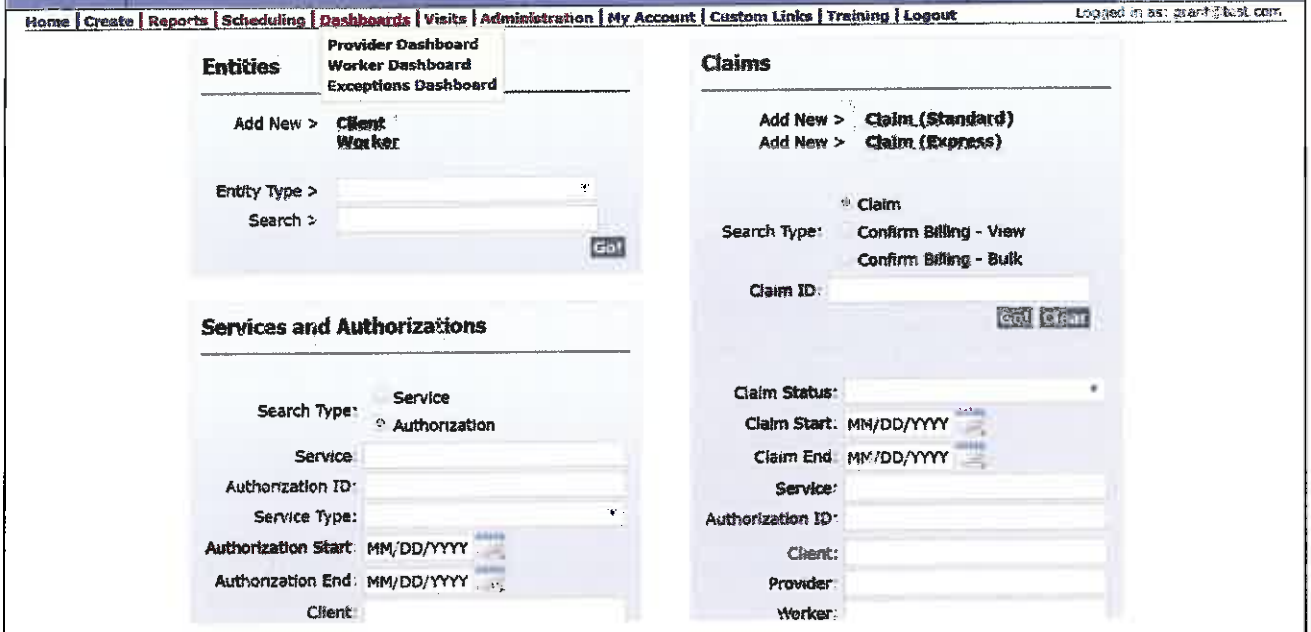


Figure 7.7 – AuthentiCare provides a user-friendly navigation for the web and mobile applications

DD076	The solution should have the ability to provide public information without requiring authentication for the web portal.	Data Sources, Delivery, & Display
FDGS will work closely with the Department to identify and publish public information on West Virginia's EVV portal. Access to the landing page will not require authentication to view this information.		
DD077	The solution should provide user interface features and capabilities including, but not limited to:	Data Sources, Delivery, & Display
DD078	Pull-down menus and window tabs	Data Sources, Delivery, & Display
DD079	Scalable, true-type screen and printing fonts	Data Sources, Delivery, & Display
DD080	Uppercase and lowercase alphabetic characters	Data Sources, Delivery, & Display
DD081	Ability to tab and mouse-click through data fields and screens	Data Sources, Delivery, & Display
DD082	Consistent theme throughout the site and standardize all headings and footers with index tabs as identified by the Department	Data Sources, Delivery, & Display
DD083	Generated messages that are clear and sufficiently descriptive to provide enough information for problem correction and be written in full English text	Data Sources, Delivery, & Display
AuthentiCare's current web interface supports the user interface features and capabilities required in DD078 – DD083. FDGS has plans in place for an upgrade to the AuthentiCare web and mobile application user interfaces. The planned upgrade will continue to support these features and capabilities with a modern look and feel as well as consistent branding, theme, and color scheme. Note that AuthentiCare reports and similar output is formatted for best fit on the printed page. Web pages are not intended for printing. The application-generated messages are full text to guide the user for resolution of data entry or edit correction. Messages are in English unless the user selects another supported language.		
DD084	The solution should provide the capability to display confirmation messages for response and request transactions when interfacing with other systems.	Data Sources, Delivery, & Display
Visit or encounter data can be uploaded in batches of up to 500 records per transaction through a secure JSON/REST web service portal. AuthentiCare will provide a response to the sender that confirms receipt or reports issues.		

Req. ID #	Requirement Text	Requirement Type
For smaller providers, visit or encounter files can be uploaded through a secure web portal. When the file import finishes, the provider can download a results file with any error messages or rejected records. Using our Custom File Layout Wizard point-and-click Designer, submitters can define their file layout so they can use their existing data exports and map their columns to our columns.		
DD085	The solution should have the ability to allow users to download or print a copy of completed submitted forms.	Data Sources, Delivery, & Display
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements once Phase 1 has been successfully implemented.		
DD086	The solution should have the ability to perform the following functions including, but not limited to:	Data Sources, Delivery, & Display
DD087	Create flags	Data Sources, Delivery, & Display
DD088	Send alerts	Data Sources, Delivery, & Display
DD089	Integration of alerts into the workflow	Data Sources, Delivery, & Display
DD090	Seamlessly integrate the generation of alerts in the workflow management process to a system user-defined group or individual	Data Sources, Delivery, & Display
We provide a series of options to define alert criteria including the target individual or individuals to automatically receive alerts through the workflow definition and management process. Please see DD032 for additional details regarding alert creation and configuration within AuthentiCare.		

7.2 Data Quality

RFP Section Attachment 8 – 3-3.1 & 4.4.2.2, pp. 120, 52
3. Data Quality
Refer to the relevant technical specifications located in Appendix 1: Detailed Specifications and pertinent narrative in Section 4: Project Specifications in this RFP to cover solution capabilities in this area.
3.1 The Vendor should describe its approach to Data Quality below. The narrative response for this category should be organized using the appropriate subject matter area as per Appendix 1: Detailed Specifications.

This sub-section describes our approach to Data Quality. AuthentiCare is scoped and meets privacy requirements, as well as HIPAA/HITECH and PHI compliance, while supporting role-based views for the state, providers, Case Managers, and Care Coordinators. AuthentiCare has a well-established record of data quality rules and integration to MMIS/MCO, resulting in 99 percent match rates for claims versus payments across multiple states. The AuthentiCare solution reduces fraud, waste, and abuse by subjecting every visit to a pre-billing claim engine workflow that applies exceptions and prevents providers from billing for incomplete or unauthorized services, preventing compliance issues before they occur.

FDGS provides additional detail to the Data Quality Subject Matter Area requirements in Table 7.5.

Table 7.5 – Detailed Response to Data Quality Requirements

Req. ID #	Requirement Text	Requirement Type
DQ001	The solution should provide a method to identify the following:	Data Quality
DQ002	National Provider Identifier (NPI)	Data Quality
DQ003	Healthcare Common Procedure Coding System (HCPCS)	Data Quality
DQ004	International Statistical Classification of Diseases and Related Health Problems, 10th revision (ICD-10) and related modifiers	Data Quality
DQ005	State-specific codes defined by the Department	Data Quality
AuthentiCare supports both provider and worker NPI. AuthentiCare is able to identify and capture additional identifiers and codes for defined services, including the identifiers and codes in requirements DQ002 – DQ005. The capture and use of these identifiers within AuthentiCare will be confirmed during the iterative Design Sessions. Service codes are configurable and AuthentiCare today supports over 70 service codes for multiple customers and as few as three for another. Services are associated with the authorization and are selectable during the check-in/check-out process to help avoid the capture of incorrect services.		
DQ006	The Vendor should collaborate with the Department to determine how data should be transferred to and from the Medicaid Management Information System (MMIS), including, but not limited to:	Data Quality
DQ007	Definition of data elements	Data Quality
DQ008	Data file formatting	Data Quality
DQ009	Data exchange frequency	Data Quality
DQ010	Thresholds for data quality and acceptance	Data Quality
FDGS agrees to collaborate with the Department through the requirements validation and iterative Design Sessions to approve the data element definitions, file format, exchange frequency, data quality edits and acceptance criteria, error processing, and other MMIS interface details. The AuthentiCare design team will begin with an MMIS interface specification from one of our most recent DXC-based interfaces. The interface specification will updated based on the		

Req. ID #	Requirement Text	Requirement Type
unique details to support the West Virginia MMIS interface.		
DQ011	The solution should allow the Department to review and approve data elements included in request and response data exchanges prior to Vendor development or configuration of the solution	Data Quality
All data exchanges will be documented within interface specifications and submitted to the Department for review and approval. Once approved, FDGS will complete the development and configuration of the interface (data exchange).		
DQ012	The Vendor should develop, publish, and maintain a system interface standard for external electronic visit verification (EVV) data partners approved by the Department.	Data Quality
AuthentiCare's system interface specifications supporting external EVV data partners will be documented and submitted for approval by the Department. Our Data Aggregator solution provides the MCOs and providers different options and capabilities to move data automatically in and out of the AuthentiCare solution so that they can choose the transport method and format most compatible with their existing systems. The process can accept data through three different channels: • Web service upload (real-time communications): Users can upload claim or encounter records for visits in batches of up to 500 records per transaction through a secure JSON/REST web service portal. Not all provider EVV systems support real-time data exchange, but AuthentiCare does. • Web portal upload: For smaller providers, claim or encounter files can be uploaded through a secure web portal. When the file import finishes, the user can download an import results file that lists any error messages or rejected records. • SFTP file gateway upload: For large providers or EVV service bureaus that produce large files, AuthentiCare can accept files through a secure SFTP gateway portal. Import results can be posted back to the same portal for subsequent pickup.		
DQ013	The Vendor should ensure that file standardization is supported for data element lengths, field format, and type.	Data Quality
As part of the AuthentiCare interface specifications for both inbound and outbound file standardization, we include all data definitions, including data element lengths, field format, data type, and valid values, as applicable.		
DQ014	The solution should incorporate a method to view interface files for investigation and further processing.	Data Quality
AuthentiCare's real-time interfaces, or web services, return success or failure to the sender as part of the API. An error listing is provided in our documentation to identify the failure so the sender can identify the resolution. Our operations staff use a combination of tools and methods including CycleView, Platinum, and other proprietary items to monitor the flow of files and that each inbound or outbound process completed successfully. The steps followed may be slightly different depending on the interface and the corresponding source and target for each file. Batch processing supports notification for failed file transfers as well as results files, providing details of success or failure. Anonymous actions like workflows and backend processing create logging and alerts for FDGS operations review. For all failed processes, FDGS operations and support staff perform recovery procedures. The Operations team is notified of failures for resolution or escalation, if required.		
DQ015	The solution should create and retain an audit trail of all interface activity in accordance with the Department's Data Retention Policy (Reference: https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2019/PO1013_DataBackup_Mar2019.pdf)	Data Quality
AuthentiCare maintains and retains a full audit trail of interface activity, including visit records, and provides a Claim History report for review. This includes the changes, who made each change, date of change, and reason codes or explanation. FDGS will maintain this audit trail in accordance with the appropriate data retention policy. However, instead of monitoring and reporting by WVOT, our data center and operations support staff are notified of any interfaces that do not complete successfully. We will then follow error processing resolution steps according to each interface specification. If appropriate, failures will be documented and reported to DHHR and the affected agency to correct the open issue.		
DQ016	The solution should make information about data exchange errors and discrepancies available to the Department and appropriate users monthly.	Data Quality
AuthentiCare exceeds this monthly requirement. Once each data exchange is completed, an import/export results file is created that shows the success or failure of the overall process and lists any discrepancies and error records with the		

Req. ID #	Requirement Text	Requirement Type
reason for the error.		
DQ017	The Vendor should provide searchable data schemas and data dictionaries for the solution	Data Quality
FDGS will review with the Department the AuthentiCare data dictionaries and searchable data schemas. Because these contain proprietary information, these reviews must be done with the proper security controls in place to prevent public release. As a SaaS offering, our policy is to protect our client's sensitive information. Allowing solution details such as our data schemas and data dictionaries to become part of the public record could create vulnerabilities. Therefore, to meet requirements involving proprietary details of the AuthentiCare solution and infrastructure, we will work with the Department to establish the appropriate security controls including a Non-Disclosure Agreement (NDA), if needed.		
DQ018	The solution should report on both duplicated and unduplicated record counts.	Data Quality
AuthentiCare incorporates data integrity checks and field edits to prevent duplicated records within its database. The team will identify duplicate records if they encounter any and report both the duplicate and unduplicated record counts in the Monthly Operations Status Report.		
DQ019	The solution should use consistent data schemes and version control.	Data Quality
AuthentiCare provides a mature database structure with consistent data schemes throughout. These are applied to the AuthentiCare modules through a stringent configuration management process to properly manage and maintain version control of the application.		
DQ020	The solution should have the ability to assure data changes made in one part of the solution automatically populate other parts of the system so as to avoid duplicate data entry.	Data Quality
With a common underlying data structure, AuthentiCare updates through the various input mechanisms, including batch and web APIs, are automatically captured for immediate use throughout the system. This approach allows other data entry pages, reports, and dashboards to access the data right away and avoids the need for duplicate data entry in other modules or components.		
DQ021	The Vendor should maintain a comprehensive list of all reports, their intended use, and business area supported.	Data Quality
AuthentiCare maintains a user manual and reports specification as part of the design documentation. This includes a list of all reports, their intended use, and supported business area.		
DQ022	The solution should generate a listing of all standard online reports available, the description of each report, and a link to the most recent report for role-based report access.	Data Quality
AuthentiCare provides a selection page listing all available standard online reports. The user can also view their most recent reports from this page. The user manual and reports specification documentation includes the description and use of each standard report. Figure 7.8 is a screen shot of AuthentiCare's main report page, where a user can request and pull reports or even set up templates of a report query they intend to use frequently.		

Req. ID #	Requirement Text	Requirement Type



Figure 7.8 – AuthentiCare's Main Report page

DQ023	The solution should identify and use consistent report fields.	Data Quality
All AuthentiCare reports include the consistent use of report fields for the respective data elements across the various reports. This consistency allows for better use of the output in business decision making.		
DQ024	The solution should display a consistent format on all reports.	Data Quality
The AuthentiCare reporting engine creates a consistent output format for all of our reports. AuthentiCare builds each report on a similarly formatted template as the default for each report. The team will work with the Department for any new reports that should result in a different output format.		
DQ025	The solution should have the ability to categorize and organize reports including, but not limited to, the following parameters:	Data Quality
DQ026	Source system	Data Quality

Req. ID #	Requirement Text	Requirement Type
DQ027	Data content	Data Quality
DQ028	Purpose	Data Quality
DQ029	Frequency	Data Quality
AuthentiCare provides default categories to organize reports by name, run time, etc. The FDGS design team will validate the categories and organization parameters with the Department to allow the capability to organize reports according to source system, data content (type), purpose, or frequency.		
DQ030	The solution should generate exception reports prior to being submitted to the receiving entity such as the Medicaid Management Information System (MMIS) or other systems receiving electronic visit verification (EVV) data to facilitate data correction by the submitting entity including, but not limited to the following:	Data Quality
DQ031	Manual edits	Data Quality
DQ032	Error corrections	Data Quality
DQ033	Additions to the interface records	Data Quality

AuthentiCare's real-time interfaces, or web services, return success or failure to the sender as part of the API. An error listing is provided in our documentation to identify the failure so the sender can determine the resolution. Batch processing supports notification for failed file transfers and results files indicate details of success or failure. Anonymous actions like workflows and backend processing create logging and alerts for FDGS operations review. For all failed processes, FDGS operations and support staff perform recovery procedures. The Operations team is notified of failures for resolution or escalation, if required. As necessary, the FDGS operations support staff will reach out to the submitting entry for resolution of exceptions.

AuthentiCare provides the ability to manually modify verification data and all modifications will be logged and maintained. We provide a manual visit verification process for DHHR when electronic visit verification is unavailable. FDGS has found that these manual scenarios are rarely necessary when using our AuthentiCare solution. We include exception reporting for claims that do not have both an electronic check-in and check-out. Exceptions must be resolved and appropriately approved by the submitting entity prior to claim submission to MMIS.

AuthentiCare's standard reports includes our Exception Report that can be filtered to include:

- All Exceptions
- All Critical Exceptions
- All Informational Exceptions
- Incomplete Visits
- Authorizations Exceptions
- Calculation Exceptions
- Eligibility Issues
- Duplicate Visits
- Visits Requiring Confirmation
- Unauthorized Locations

Req. ID #	Requirement Text	Requirement Type



Figure 7.9 – Sample of an AuthentiCare Exception Report Header

Visits with critical exceptions are held in the system for the provider to review and make corrections, while those with no exceptions or only informational exceptions are staged for provider approval.

Edits and Corrections: AuthentiCare makes it easy for Providers to address errors and exceptions that do occur. The system provides an Exception Dashboard that breaks critical exception visits (those that are currently non-billable) into separate categories for any date of service range.

A single click of a button on the Exception Dashboard takes the provider directly to a summary list of visits with that exception for the provider to quickly drill down and make the necessary corrections.

DQ034	The solution should generate error reports at the summary and detail levels that include all data necessary to resolve errors monthly and as requested by the Department.	Data Quality
As noted in DQ030 – DQ033, AuthentiCare has a thorough exception reporting capability. In addition, data quality of information exchanged between systems is also reported. When each data exchange is complete, an import/export results file is created that shows the success or failure of the overall process and lists any discrepancies and error records with the reason for the error. This report includes the detailed error for each record. Error resolution steps, and onboarding any entity that will exchange data with AuthentiCare, are part of the training.		
DQ035	The solution should store reports to allow users the ability to retrieve them quickly per the Department's business rules.	Data Quality
AuthentiCare stores previously run reports for authorized users to quickly retrieve in the future. As reports are run, the View Reports list in Figure 7.8 – AuthentiCare's Main Report page (above) is refreshed for quick access according to the Department's business rules.		
DQ036	The solution should reload or resend records if they have not been applied correctly to the receiving entity.	Data Quality
Records that have caused an error previously will be corrected by FDGS or the submitting entity and reloaded/resent to the receiving entity according to the respective error processing defined in the interface specification.		
DQ037	The solution should detect duplicate files or records and isolate them for manual review and further processing.	Data Quality
For each data exchange (inbound or outbound), AuthentiCare processes will verify that duplicate files or duplicate records are not accepted into the EVV system. If appropriate, a pre-edit check or manual review of files or records will be conducted and the steps for resolution completed prior to further processing. These checks and resolution steps are part of the interface specification and included in the AuthentiCare operations handbook.		
DQ038	The solution should create messages that accurately describe errors received as a result of a data transfer.	Data Quality
AuthentiCare data exchange processes include descriptive messages to identify and resolve the different error scenario encountered during the data transfer.		
DQ039	The solution should have the ability to maintain an up-to-date inventory of all forms utilized and make this inventory available to the Department upon request.	Data Quality
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		

Req. ID #	Requirement Text	Requirement Type
DQ040	The solution should have the ability to identify which fields in forms are required and which are optional.	Data Quality
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DQ041	The solution should have the ability to store the date that a correspondence was delivered for printing in a preferred date format of MM/DD/YYYY.	Data Quality
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DQ042	The solution should provide automatic default file naming convention for saved correspondence as agreed upon with the Department.	Data Quality
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DQ043	The solution should categorize and classify types of correspondence as agreed upon with the Department.	Data Quality
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
DQ044	The solution should distinguish between, and incorporate, business days, weekends, and state holidays in all time-related functions in the system.	Data Quality
AuthentiCare is designed to capture EVV on any day of the week as well as holidays. Since caregivers will be providing services on all days, AuthentiCare will be available to serve them and the beneficiaries. Alerts for late and missed visits will be delivered regardless of day to assist in engaging back up caregivers as appropriate. Reports will run as scheduled and be available for the requester upon their next work day.		
DQ045	The solution should include web-based online help functionality in searchable portable document format (PDF) that includes a searchable database of common problems.	Data Quality
AuthentiCare's web-based online help function is available via our comprehensive User Manual, which resides within the application itself. The User Manual is a searchable PDF document which includes step by step instructions for every module and Frequently Asked Questions (FAQs).		
DQ046	The solution should set parameters on fields to prevent system users from entering information outside of those parameters.	Data Quality
AuthentiCare incorporates field edits as well as drop-down lists to allow only specific data values into the system. The FDGS team will review these with the Department during the iterative Design Sessions to validate the edits and valid values specific to the West Virginia EVV rules and policies.		
DQ047	The Vendor should produce all member- and provider-facing content written at no greater than an eighth grade reading level.	Data Quality
Our content, training materials, and related documentation take into account low literacy levels of members or providers that may use AuthentiCare. FDGS has previously provided materials at a fourth or fifth grade literacy level to provide for easy understanding and comprehension of the needed EVV features and functions.		
DQ048	The solution should include email addresses in the authorization table for registration, and email addresses should be kept confidential and only used for official Department business.	Data Quality
AuthentiCare captures and securely maintains email addresses during the user registration process. These are kept confidential and will only be available for official Department business.		

7.3 Hardware and Infrastructure

RFP Section Attachment 8 – 4-4.1 & 4.4.2.3, pp. 120, 52
4. Hardware and Infrastructure
Refer to the relevant technical specifications located in Appendix 1: Detailed Specifications and pertinent narrative in Section 4: Project Specifications in this RFP to cover solution capabilities in this area.
4.1 The Vendor should describe its approach to Hardware and Infrastructure below. The narrative response for this category should be organized using the appropriate subject matter area as per Appendix 1: Detailed Specifications.

This sub-section describes our approach to Hardware and Infrastructure. AuthentiCare is built on a modern infrastructure and hosted in our world-class data centers to support integration with open standards and the most current platforms. FDGS provides additional detail in this sub-section to meet the mandatory requirements listed in Table 6.4 as part of RFP Attachment 6 – Mandatory Requirements.

Table 7.6 – AuthentiCare meets all mandatory requirements for Hardware and Infrastructure

Met	Req ID #	Requirement Text
☑	MR003	The Vendor must ensure that solution modules and applications integrate successfully and effectively with minimal or no customization.

The AuthentiCare EVV solution architecture is based on a Service Oriented Architecture (SOA), which is beneficial for multiple system integrations. AuthentiCare web services are available for other customer-approved systems external to EVV. FDGS adopted SOA to meet our customers' current and future business requirements while maintaining security, scalability, reliability, and availability expectations.

Our focus is to support an expedited implementation period that includes minimal or no customization to the AuthentiCare EVV solution. Through iterative design and configuration sessions, we will be able to implement an EVV solution that is compliant with the 21st Century Cures Act and prepare the Department for CMS certification beginning with the Operational Readiness Review (ORR).

Once the critical functionality is deployed and the system acceptance from the Department is attained, FDGS will work with DHHR to plan for additional design and configuration sessions to expand on the EVV features and functions available to your provider community, Department staff, and other stakeholders.

FDGS provides additional detail to the Hardware and Infrastructure Subject Matter Area requirements in Table 7.7.

Table 7.7 – Detailed Response to Hardware and Infrastructure Requirements

Req. ID #	Requirement Text	Requirement Type
IN001	The solution should have the ability to support various current technologies for data interchange and electronic visit verification (EVV) data submission and verification including, but not limited to, web portal, application interface, telephony, quick response (QR) codes, and automated location verification.	Hardware and Infrastructure
AuthentiCare supports multiple technologies for data exchange based on the latest technologies and industry standards. AuthentiCare's service endpoints, APIs, and web services will be exposed for both inbound and outbound		

Req. ID #	Requirement Text	Requirement Type
interfaces. Data exchange can be done in batch mode as well as the web services and APIs. AuthentiCare offers multiple technology options for the data collection necessary to verify visit information. Our hosted solution includes web, mobile, and IVR (telephony) to fully cover all statewide EVV activities. The business processes in AuthentiCare automatically verify the time, location, and task performance activities. Our various technology options provide an automatic backup option if there are network or system outages. These options also afford service providers and clients choices based on their preferences and unique needs. AuthentiCare also supports QR cards as an alternative. However, the combination of web, mobile, and IVR can meet the Department's requirements for visit verification.		
IN002	The Vendor should utilize open architecture standards and scalability to promote integration throughout the West Virginia technology enterprise.	Hardware and Infrastructure
The AuthentiCare EVV solution architecture is based on open architecture standards, including Service Oriented Architecture (SOA). These standard web services and APIs are available for other customer-approved system consumption external to EVV. FDGS adopted open standards and SOA to meet our customers' current and future business requirements while meeting security, scalability, reliability, and availability requirements. The AuthentiCare solution can be integrated into a bigger SOA architecture using data interfaces and APIs and accessed by any Medicaid enterprise application that has need of our services through the Enterprise Service Bus (ESB) client. AuthentiCare EVV processes employ data interchange and web service standards, including secure JSON API and restful (REST) web services.		
IN003	The solution should be flexible and readily adaptable to changing Department and federal requirements and as requested by the Department	Hardware and Infrastructure
AuthentiCare uses a modular, flexible, and readily adaptable approach to systems development. This includes the use of open interfaces and exposed application programming interfaces (APIs) to separate business rules from core programming. It also makes business rules available in both human and machine-readable formats. Most business rules in AuthentiCare are captured in metadata tables in the database so they are easily changed and updated as EVV policy and business rules change at both the state and federal levels.		
IN003A	The solution should address the disruption or limited availability of network connectivity, telephony, and/or cell coverage at the visit site by providing members and providers more than one method to send and receive electronic visit verification (EVV) data.	Hardware and Infrastructure
AuthentiCare offers multiple technology options for the data collection necessary to verify visit information. Our hosted solution includes web, mobile, and IVR (telephony) to fully cover all statewide EVV activities. The AuthentiCare mobile app is the most comprehensive option for capturing EVV data, and it is backed up by web entry, IVR (telephony), and our Store and Forward capabilities when network connectivity is unavailable.		
IN003B	The solution should have the ability to capture and retain electronic visit verification (EVV) data gathered when the transmission services are offline for any reason at the visit site and to send or receive queued system data when services are restored.	Hardware and Infrastructure
In limited service areas, the AuthentiCare mobile app provides Store and Forward technology features. We understand that, in many care locations, limited or poor cellular data service exists at the place of service. The AuthentiCare mobile app captures the time and GPS location of service in the app at the time and place service is delivered. The information is uploaded and recorded in the online system when the caregiver carries the device to a location that has Wi-Fi or cellular data service. The iOS and Android AuthentiCare mobile applications have a page banner that turns red when there is no data connection or the device is in airplane mode. The banner turns white when the device reestablishes a data connection, so that the user can tell when data services are available. With Store and Forward capability, the mobile device time and location services are used for EVV.		
IN004	The solution should provide archival and purge processes that do not degrade performance or interrupt the system.	Hardware and Infrastructure
AuthentiCare will support archival and purge processes while maintaining agreed-upon performance levels and avoiding any interruption to the system.		
IN005	The solution should allow centralized deployment of system updates and system maintenance.	Hardware and Infrastructure
Our approach to configuration management and hosting of the AuthentiCare application provides the capability for centralized deployment of system updates and system maintenance.		
IN006	The solution should provide workflow functionality that supports a variety of mechanisms to initiate, execute, suspend, or terminate workflows including,	Hardware and Infrastructure

Req. ID #	Requirement Text	Requirement Type
	but not limited to:	
IN007	Communication events (email, document upload, form submissions, or phone)	Hardware and Infrastructure
IN008	System-generated events	Hardware and Infrastructure
IN009	User-triggered events	Hardware and Infrastructure
IN010	Exception-processing events	Hardware and Infrastructure

AuthentiCare delivers the ability to configure automated workflow events that may result in alerts, such as when services are late or missed, so a qualified back-up worker may be dispatched. This flexible workflow capability may result in different event actions like communication or email, system-generated alert, user-triggered event, or the creation of exceptions and escalation notifications. AuthentiCare is able to logically initiate, execute, suspend, or terminate workflows based on predecessor actions within the system or based on specific user interaction.

Automated alerts may be sent via email to designated recipients as determined by Department policy. Support coordinators, provider agencies, emergency back-up workers, or State staff may be notified that a critical service has not been delivered.

Alerts or other system events may be configured to meet the requirements of individual services or programs as driven by DHHR policy. For example, some communication events caused by data aggregator input processing may result in alerts sent to multiple recipients as defined in the configuration template. These alerts can be tracked by caregiver, by provider, or by recipient in various reports and dashboards to identify trends that need to be addressed.

IN011	The solution should include definition and modeling of workflow processes and their constituent activities.	Hardware and Infrastructure

The AuthentiCare workflow and business rules engine is configured using a web-based tool for managing the plug-in workflow modules. Workflow processes and their constituent activities will be fully documented, defined, and modeled within our system documentation. FDGS will review the workflow and business rules as part of the requirements validation and iterative Design Sessions.

Workflow modules perform key business rule tasks, primarily in four categories, including matching and status, calculations, critical exceptions, and informational exceptions. Working with our customers and their waiver and non-waiver rules, FDGS has built a library of configurable workflow plug-ins that encompass the most common Medicaid business rules for processing visits.

IN012	The solution should have the ability to facilitate mass email notifications.	Hardware and Infrastructure

AuthentiCare does not currently support mass email notifications. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.

IN013	The solution should have the ability to reissue and track any correspondence or form as requested by the Department.	Hardware and Infrastructure

AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.

IN014	The solution should have the ability to schedule any report to be run at varying levels of frequency or on-demand.	Hardware and Infrastructure

The main reports engine web page provides easy access to run on-demand reports, as well as create and schedule regular reports for re-use, and then pick up completed reports in the user's preferred format (including PDF, Excel, CSV, and XML). The system allows the user to schedule or submit report requests, do other work while the reports run, and then come back to the page to pick up the reports when they are ready.

IN015	The solution should provide integrated print capability within the application for any report.	Hardware and Infrastructure

AuthentiCare provides integrated print capability within the application for any report.

Req. ID #	Requirement Text	Requirement Type
IN016	The solution should have the ability to notify users of system maintenance and other information approved to be distributed by the Department.	Hardware and Infrastructure
FDGS provides a Customer Care Plan that describes ongoing communication and customer support throughout the life of the contract. The Project Manager will work with DHHR to identify the stakeholders that should be notified of different system updates. The project team uses the communication list to notify users of upcoming EVV system maintenance and "what's new" for each approved release of system updates, as well as notifications of system downtime due to planned updates and scheduled maintenance, and other approved information from the Department.		
IN017	The Vendor should manage, track, and report on user support services via multiple channels, including:	Hardware and Infrastructure
IN018	Telephone	Hardware and Infrastructure
IN019	Member portal	Hardware and Infrastructure
IN020	Email	Hardware and Infrastructure
IN021	Mail	Hardware and Infrastructure
AuthentiCare will support the management, tracking, and reporting of support services via multiple channels, including telephone or email. FDGS will work with the Department to identify the most efficient channel and the details to be tracked. FDGS does not currently support requests through web (member portal) or mail. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
IN022	The Vendor should provide investigative results inclusive of mitigation measures to address reported incidents within 30 days of the documented incident.	Hardware and Infrastructure
FDGS agrees to provide investigative results, inclusive of mitigation measures, to address reported incidents within 30 days of the documented incident.		
IN023	The Vendor should support provider compliance through direct assistance, coaching, technical assistance, and other active outreach activities as requested by the Department.	Hardware and Infrastructure
To support provider compliance, FDGS provides thorough training and outreach as part of the overall Training and Outreach Plan. We offer multiple training and outreach options including direct assistance, coaching, technical assistance, and other active outreach activities. The AuthentiCare outreach and training materials include a comprehensive set of user training elements that we expand and to which we add deliverables over time to support compliance from the ever-changing provider community. FDGS options for training include our provider forums and assistance calls. The Account Manager will take the lead in hosting post-implementation provider forum calls. Initially, provider forum calls occur at least weekly—typically for one to three months or until experience and comfort is established among the provider community—then taper down to a monthly schedule. The provider forum offers an opportunity for ad hoc training sessions where attendees ask questions and receive answers to issues they are currently experiencing. The forums also afford an active outreach opportunity for stakeholders to receive clear communication and understanding of needs and requests that may lead to enhancements to the AuthentiCare solution, and that may better equip and support the provider community in the ongoing compliance with the 21st Century Cures Act.		
IN024	The solution should provide users a description of the minimum hardware and software requirements, installation, maintenance, and enhancement of software based on role and system requirements prior to system updates.	Hardware and Infrastructure
FDGS agrees to provide users a description of the minimum hardware and software requirements, however, as a fully hosted, web-based, and mobile offering, the browser version is most likely the only check for end users.		
IN025	The solution should allow users to schedule and modify system events as requested by the Department.	Hardware and Infrastructure
AuthentiCare supports the scheduling and modification of system events. The details for the manipulation of system events will be confirmed in the requirements validation and design phase of the EVV project.		
IN026	The Vendor should provide a technical support call center located within the contiguous United States.	Hardware and Infrastructure

Req. ID #	Requirement Text	Requirement Type
The technical support call center for AuthentiCare is based in Hagerstown, Maryland.		
IN027	The solution should document call information, as agreed upon by the Department.	Hardware and Infrastructure
Prior to Go-Live, the Account Manager will provide a sample of our Monthly Operations Status Report showing the current format and content of call information. The statistics and their presentation within the Monthly Operations Status Report for DHHR will be validated so that the agreed-upon metrics are tracked and reported consistently from the start of the Maintenance and Operations of the EVV project.		
IN028	The technical support call center hours of operation should be Monday through Friday, from 9:00 a.m. to 6:00 p.m. Eastern Time (ET) and on an emergency basis as requested by the Department. The call center may be closed for standard federal holidays and West Virginia State holidays.	Hardware and Infrastructure
Our Help Desk approach fully supports the RFP requirements for technical support. The Help Desk is easily accessible via email and telephone and is committed to being our customers' valued business partner in support of the AuthentiCare product and support services, making sure we comply with our customers' requirements and provide provided within one day of receipt. Support representatives are cross-trained to provide full coverage and are available 24 hours a day, 7 days a week.		

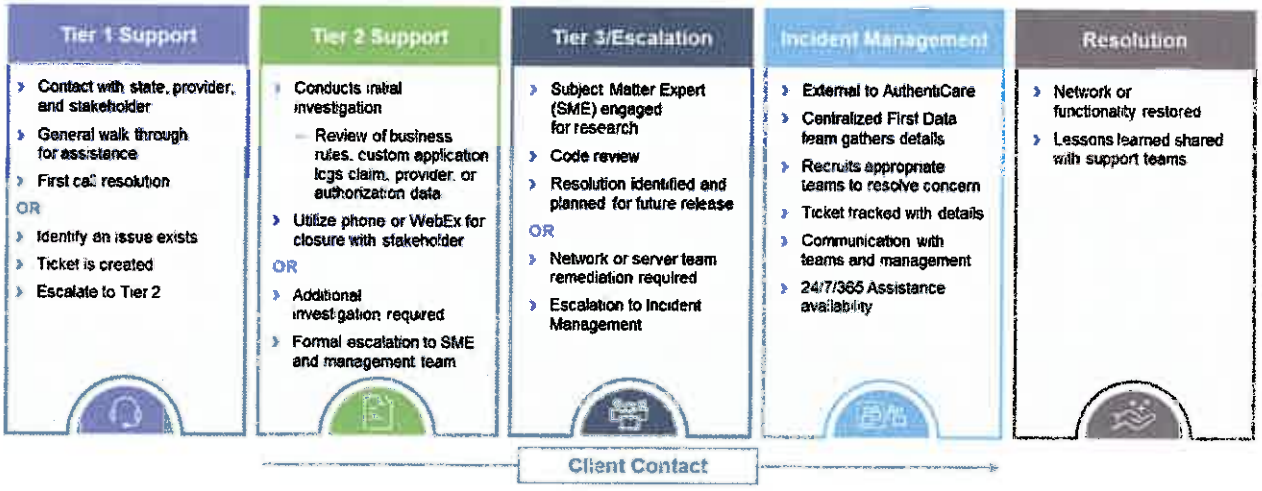


Figure 7.10 – FDGS offers a tiered approach to client support and services

Our tiered support team staff confirms that the proper attention is given to the needs of the client. The Tier 1 call center is staffed during standard business hours 9:00 AM – 6:00 PM Monday through Friday, Eastern Time, excluding holidays. The Tier 1 Call Center Representatives are the first line of contact for providers to reset passwords, research claims, review authorizations, and create tickets. These representatives provide minor training and education, and work with providers to address simple or user-related issues. They have the ability to answer questions about check-in/out issues, case manager relationships, schedules, reports, and other concerns related to AuthentiCare.

Items that require advanced assistance or calls outside of the core hours are handled by the Tier 2 Help Desk Specialist Team. Tier 2 Help Desk Specialists have a strong understanding of the application and strong compliance requirements for our customers. They have the ability to research reported concerns through application log research; review of Authorizations, Provider, Client, and Claim files; determine authorization issues; and provide in-depth troubleshooting of AuthentiCare software and systems. In some instances, client concerns that reach the Tier 2 Help Desk Specialists are used for training purposes to educate the call center and client alike to promote knowledge sharing.

Tier 3 AuthentiCare Subject Matter Experts are experts from various departments who are available to Tier 1 and Tier 2 staff members as an escalation point on advanced issues. They provide advanced data research capabilities and the analysis needed to review relationships and outcomes based on business rule and application code functionality. Tier 3 resources are assigned to issues when needed through a formal escalation process.

IN029	The Vendor should return all after-hour calls by the next business day, in the caller's preferred language and/or through oral interpretation services. (Reference: https://www.hhs.gov/civil-rights/for-individuals/section-	Hardware and Infrastructure

Req. ID #	Requirement Text	Requirement Type
	1557/translated-resources/index.html	

FDGS realizes that problems and technical issues do not limit themselves to normal business hours, which is why a Tier 2 Help Desk Specialist is on call 24x7 to resolve or escalate issues that occur outside of standard business hours. A call to the support number outside of standard business hours will be routed to a Tier 2 Help Desk Specialist to support evenings, weekends, and holidays for technical application concerns.

Our goal is to exceed this next business day requirement where most after-hour calls are returned within 10 minutes. If necessary, language translation or interpretive services are available.

Table 7.8 – Outside Standard Business Hours for Help Desk Support

Outside Standard Business Hours 6:00 pm – 9:00 am Monday through Friday, weekends, and holidays
1. Dial the support number 800-441-4667 and your call will be forwarded immediately to the Tier 2 Help Desk Specialist on Call. 2. The On-Call Specialist will answer the call. If you need to leave a message, your call will be returned within 10 minutes. 3. If the issue is a Severity 1 or 2 and has significant impact on your ability to conduct your business, the On-Call Specialist will IMMEDIATELY contact the Account Manager and Help Desk Director. We also have an Incident Management team ready to contact the appropriate essential personnel to effectively work the issues as a Top Priority regardless of the hour. 4. The Customer is contacted within 30 minutes of communicating with the Specialist with an update and ticket number plus any other pertinent information as appropriate.

The Client Support Help Desk is dedicated to tracking and resolving client concerns as quickly as possible. To help manage incident reporting and resolution, each incident interaction from DHHR personnel is logged into a centralized ticketing system that is managed by the Support Help Desk.

IN030	The Vendor should provide functionality to manage calls to the Technical Call Center including, but not limited to:	Hardware and Infrastructure
IN031	Creation of tickets	Hardware and Infrastructure
IN032	Editing existing tickets	Hardware and Infrastructure
IN033	Sorting of call center ticket information	Hardware and Infrastructure
IN034	Filtering of call center tickets or electronic records	Hardware and Infrastructure

FDGS will establish and maintain a specific EVV Customer Care Plan for the Department that addresses all aspects of AuthentiCare customer care services, including our help desk coverage solution. FDGS has been operating client support call centers for over 35 years and uses industry standards for staffing, quality, and metric delivery.

The client support call center for AuthentiCare includes a modern ticketing system that captures every call in detail. Our support staff are able to create, edit, sort, and filter ticket details to quickly retrieve and resolve and report on related metrics throughout the maintenance and operations of AuthentiCare.

IN035	The Vendor's Technical Call Center should have the ability to track data including, but not limited to:	Hardware and Infrastructure
IN036	The caller	Hardware and Infrastructure
IN037	The question(s) and/or issue(s)	Hardware and Infrastructure
IN038	The Vendor staff responding to the ticket	Hardware and Infrastructure
IN039	The date(s)	Hardware and Infrastructure

Req. ID #	Requirement Text	Requirement Type
IN040	The time(s)	Hardware and Infrastructure
IN041	The status (opened or closed)	Hardware and Infrastructure
IN042	Problem resolution	Hardware and Infrastructure

FDGS will collaborate with DHHR to finalize and approve tracking data—including the caller details, question content and related details about the issues—and support technicians and their notes, data and time, current status of each ticket, and the historical details of the findings and ultimate resolution. Each issue is also assigned a severity and priority to maintain the proper focus by the support technicians. These definitions are included in the agreed-upon performance metrics and resolution targets. Our operations and support teams monitor the timeliness and effectiveness of their online and telephonic user support using performance metrics and targets. We incorporate performance metrics into the Monthly Status Reports.

- **Customer Support Metrics Management:** We review Customer Care and Support metrics monthly to identify opportunities for improvements.
- **Ongoing Review of Customer Service Delivery:** Ongoing review of customer service delivery statistics verifies that processes and staffing levels are adjusted appropriately to confirm customer satisfaction with Client Services Help Desk.
- **Customer Interaction Report:** We generate a Client Interaction Report each month presenting the volume of calls handled through the Client Services Help Desk.
- **Metrics Data Collection:** FDGS will use a combination of monitoring tools and ad hoc data elements collected from the AuthentiCare database along with information tracked from various internal data sources.
- **Scorecard Metrics Management:** Includes a summary of work activities and major accomplishments achieved during the reporting period, in addition to any problems or issues that require management attention.

AuthentiCare automated monitoring checks the application every 15 minutes every day of the week. This test validates the proper operation of AuthentiCare. If the test encounters an anomaly, it transmits an error message to the FDGS Help Desk Tier 2 Technician for analysis. Our Tier 2 Technicians proactively monitor the AuthentiCare application's daily operating statistics. A checklist of expected processing will be used to monitor that all processes are executed properly. Infrastructure monitors on the servers and database continually monitor memory, CPU, and disk usage, along with any system or database server errors.

IN043	The Vendor's Technical Call Center should have the ability to repeat call options automatically.	Hardware and Infrastructure

Callers always have the option to repeat menu options as many times as needed. FDGS will review the menus and scripts with the Department prior to Go-Live.

IN044	The Vendor should maintain sufficient staff and telephone lines to perform all required technical support call center functions.	Hardware and Infrastructure

The AuthentiCare technical support call center is designed to scale up to meet increased demand; especially during the first few months following Go-Live. FDGS has more than sufficient staff and telephony capacity for the support of AuthentiCare users in West Virginia.

IN045	The solution should use automated menus, including an easily accessible option for reaching a live operator.	Hardware and Infrastructure

Callers will be provided with an easily accessible option to reach a live operator during normal support hours.

IN046	The solution should provide assistance to inquiries received from persons who require special assistance including, but not limited to:	Hardware and Infrastructure
IN047	Persons with Limited English Proficiency (LEP)	Hardware and Infrastructure
IN048	Persons with vision disabilities	Hardware and Infrastructure
IN049	Persons with hearing disabilities	Hardware and Infrastructure
IN050	Persons with speech disabilities	Hardware and Infrastructure

The AuthentiCare support model provides assistance to those needing special assistance including persons with Limited English Proficiency (LEP), vision disabilities, hearing disabilities, or speech disabilities. Our Account Manager

Req. ID #	Requirement Text	Requirement Type
will coordinate with our support teams for any other scenarios that may result in different support options.		
IN051	The solution should include an online option for users to report any technical problems.	Hardware and Infrastructure
Technical issues can also be reported through sending an email to AuthentiCare.Support@FirstData.com. For critical issues, FDGS recommends attempting to contact the Client Services Help Desk prior to sending an email.		
IN052	The Vendor should ensure the solution components that are web based have cross-browser compatibility over the life of the contract and support software utilization in the current version and two (2) prior versions at a minimum for the following browsers including, but not limited to:	Hardware and Infrastructure
IN053	Microsoft Edge	Hardware and Infrastructure
IN054	Apple Safari	Hardware and Infrastructure
IN055	Google Chrome	Hardware and Infrastructure
IN056	Mozilla Firefox	Hardware and Infrastructure
IN057	Microsoft Internet Explorer	Hardware and Infrastructure
AuthentiCare's web application supports each of these web browsers including Microsoft Edge, Apple Safari, Google Chrome, Mozilla Firefox, and Microsoft Internet Explorer. Upon contract execution, FDGS will verify the current browser releases available at that time and verify compatibility with the two prior versions of each browser, respectively. Our development and testing teams confirm browser compatibility regularly as new releases are made available.		
IN058	The solution should incorporate a non-restrictive environment for experienced users to directly access a screen or to move from one screen to another without reverting to the menu structure.	Hardware and Infrastructure
AuthentiCare provides intuitive navigation in both the mobile and web applications. Direct navigation or "fast path" is not available. AuthentiCare screens navigate to the next page or window with relevant detail based upon the prior screen. Navigation is driven by application logic, business rules, and workflow.		
IN059	The solution should generate drop-down lists to identify options available, valid values, and code descriptions by screen field.	Hardware and Infrastructure
AuthentiCare provides automatic lookup and auto-population of some fields. To maintain data integrity, fields that allow a limited list of valid values use drop-down structures so that users can only select valid entries. Codes and code descriptions are available for each screen field, where applicable.		
IN060	The Vendor should provide web applications that satisfy the Priority 1 Checkpoints from the Web Content Accessibility Guidelines 1.0 developed by the World Wide Web Consortium (W3C), as detailed at: http://www.w3.org/TR/WCAG10/full-checklist.html.	Hardware and Infrastructure
AuthentiCare is accessible and compliant with ADA, Section 508, and WCAG 2.0 standards. AuthentiCare is able to demonstrate substantial W3C compliance, as well as the capability to use screen-reading software, like JAWS® or ZoomText®. With regard to accessibility standards, FDGS has engaged Level Access to advise us on accessibility and use with assistive technology for the AuthentiCare Web and Mobile App. Level Access has provided third-party ADA Section 508 certification of both the Web and Mobile applications. Copies of the most recent AuthentiCare VPAT 508 test report will be evidence included in the ORR EVV criteria EVV8 Americans Disability Act compliance.		
IN061	The solution should have the ability to include secure and public facing tabs for the web portal.	Hardware and Infrastructure
The AuthentiCare web application only supports secure access to pages and tabs. We will work with the Department to identify if some public notifications and messaging can be placed on the login page. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
IN062	The solution should have the ability to utilize an authentication process to handle multiple layers of security levels as requested by the Department.	Hardware and Infrastructure
AuthentiCare's web, and mobile, and IVR modules employ two-factor authentication preventing unauthorized access to the application, and visit data, and any mobile device. Access to AuthentiCare environments is carefully restricted to		

Req. ID #	Requirement Text	Requirement Type
only necessary staff. Staff must individually authenticate to each server with a public/private key pair in order to access AuthentiCare environments. In addition to user name and strong password, the AuthentiCare web will use a time-sensitive, one-time PIN, while the mobile app will use user name and password along with the device ID.		
IN063	The solution should have the ability to provide self-service password resets and mask the display of passwords at the sign-on screen when the user enters the portal.	Hardware and Infrastructure
AuthentiCare supports self-service password resets and will use a standard data entry mask of the password when entered by the user.		
IN064	The solution should have the ability to mask the display of passwords at the sign-on screen when entered by the user.	Hardware and Infrastructure
AuthentiCare will use a standard data entry mask of the password when entered by the user.		
IN065	The Vendor should ensure that web portal field definitions comply with system field definitions.	Hardware and Infrastructure
FDGS will verify that all AuthentiCare web application field definitions comply with system field definitions.		
IN066	The Vendor should, for the web portal, provide Internet security functionality to include firewalls, intrusion detection, and encrypted network/secure socket layer (SSL).	Hardware and Infrastructure

AuthentiCare provides a modern, secure, hosted web solution that includes the latest security functionality including application protection using firewalls and intrusion detection, as well as encryption of data both in transit across the network and at rest.

Firewall

FDGS' dedicated Application Security Assessment team routinely reviews AuthentiCare. Code is scanned statically and dynamically for a broad scope of vulnerabilities including OWASP Top 10, cross-site scripting, and SQL injection. Our Web Access Firewall (WAF) proactively reviews access activity, files in motion, malformed requests, and denial of service.

Intrusion Protection

Intrusion Detection is in place on the following segments: Internet point-of-presence, DMZ, extranet, internal production network, and network segment hosting target data. It is configured to generate alerts in case of incidents and values exceeding normal thresholds for the environment. A formal process is in place to regularly update the Intrusion Detection System (IDS) signatures based on new threats and changes in the environment. The system is electronically monitored 24x7x365. IDS events feed into the Incident Management process that alerts operations personnel to take action to resolve the issue.

In addition to monitoring network connections and incoming traffic, FDGS also maintains and monitors a Data Loss Prevention (DLP) system to prevent egress of network data and email traffic containing PII. This additional check on outgoing flow of specific types of data offers additional protection by preventing specific data from leaving our secure environment.

Encryption of Data in Transit (Network/SSL layer)

Please see details included in IN067.

IN067	The Vendor should provide and maintain a secure data storage solution that includes encryption of data in transit and encryption of data at rest.	Hardware and Infrastructure

Encryption of Data at Rest

The AuthentiCare platform provides separate databases behind firewall storage for each customer's data. In a 2019 platform upgrade, AuthentiCare began providing column-level encryption of PII and PHI data at rest using Voltage® encryption tools. This applies to both database and file storage. Column-level encryption replaces storage-level encryption that was the previous standard. Data at rest on the AuthentiCare Mobile app in both Apple® and Android® environments is AES 256-bit encrypted using the key from the AuthentiCare server with a random salt. Mobile passwords are stored in the AuthentiCare portal and compared as an SHA 512-bit encrypted hash, so that only the Mobile user knows the pass phrase used to generate the hash.

Encryption of Data in Transit

For all web and web service connections to the AuthentiCare platform, including mobile transactions, FDGS requires TLS 1.2 Transport Level Security. The mobile apps employ certificate pinning for resistance to "man in the middle" attack. File transfers use the FDGS File Gateway hosted SFTP site, and are AES 256-bit encrypted according to FIPS 140-2 requirements.

7.4 Security Management

RFP Section Attachment 8 – 5-5.1 & 4.4.2.4, pp. 120, 53
5. Security Management
Refer to the relevant technical specifications located in Appendix 1: Detailed Specifications and pertinent narrative in Section 4: Project Specifications in this RFP to cover solution capabilities in this area.
5.1 The Vendor should describe its approach to Security Management below. The narrative response for this category should be organized using the appropriate subject matter area as per Appendix 1: Detailed Specifications.

This sub-section describes our approach to Security Management. FDGS provides additional detail in this sub-section to meet the mandatory requirements listed in Table 7.9 as part of RFP Attachment 6 – Mandatory Requirements.

FDGS and Fiserv have a corporate-wide focus on information security, including maintaining compliance of our respective products and services across a complex set of laws, regulations, guidelines, and clients. As defined by NIST, information security is "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction."

FDGS achieves these goals by:

- Assigning experienced security staff with practical experience in performing multiagency security review
- Assessing the in-scope security controls using the same criteria and processes as those used by external auditors

This approach reduces risk of adverse security events caused by missing or defective security controls, and reduces the risk of unexpected audit findings and the need for subsequent unplanned corrective actions.

In the AuthentiCare EVV system solution, Medicaid data necessary to perform the duties as outlined in this RFP are stored in a secure and confidential manner that meets Health Insurance Portability and Accountability Act of 1996 (PL 104-191) (HIPAA) requirements. This includes HIPAA requirements related to privacy, security, transaction code sets, and medical provider enumeration.

On an ongoing basis, Fiserv's policies are reviewed and approved by three broadly recognized assessors—SSAE-18/SOC 1 (Ernst & Young), PCI DSS (Trustwave), and GLBA (Federal Financial Institutions Examination Council [FFIEC])—in addition to many state, local, and customer assessors. Fiserv has established a Global Cyber Security Policy that aligns with the NIST CSF (National Institute of Standards and technology, Cyber Security Framework), which is based on a subset of controls within the comprehensive NIST SP 800-53 r4 controls. The Global Cyber Security Policy is fully complementary to the ISO (International Standards organization) 27001-2013 cyber security controls, with certain geographic areas maintaining ISO 27001-2013 certification. Corporate security policies also include practices in FTC 16 CFR Part 314, Standards for Safeguarding Customer Information; Final Rule. Certified PCI-DSS and SSAE 18 controls at Fiserv map to and cover the applicable HIPAA security controls as specified in NIST SP800-66 r1 Appendix D: *HIPAA Security Rule Standards and Implementation Specifications Crosswalk*.

Data integrity, privacy, and protection are a vital component of any EVV solution. AuthentiCare scopes provider and beneficiary data and meets the privacy regulations and requirements of

HIPAA/HITECH and PHI while supporting role-based views for the state, providers, Case Managers, and Care Coordinators.

We maintain a documented security plan that is regularly audited by the FFIEC, our Payment Card Industry (PCI) assessor, and under SSAE-18 by Ernst and Young. Fiserv security plans and procedures are prepared at a facility level, and the solution is hosted in large-scale, redundant data centers with DHHR data housed separately from other customers' data.

Our security plan is fully matured and in operation today. The plan encompasses the full AuthentiCare platform environment including both our primary and secondary (backup) facilities. FDGS verifies that all Medicaid data necessary to perform the duties as outlined in this RFP are stored in a secure and confidential manner that meets federal and state rules and regulations, including HIPAA compliance.

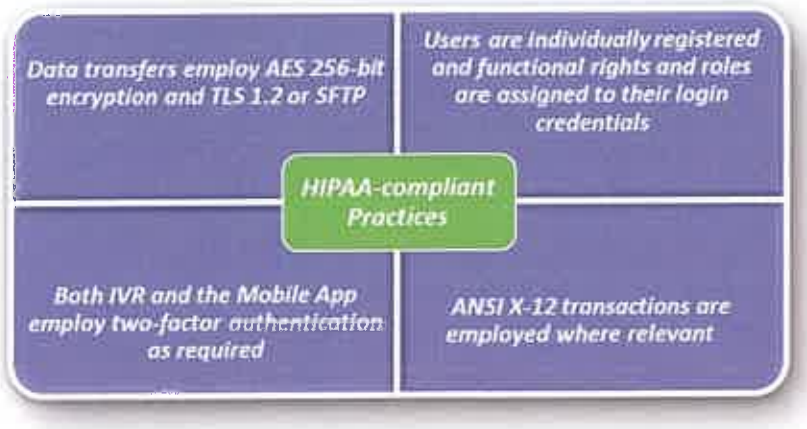


Figure 7.11 – FDGS' HIPAA-compliant practices

FDGS understands the necessity of protecting the privacy and confidentiality of your data. The EVV system meets the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Our HIPAA-compliant practices are displayed in Figure 7.11. Our solution processes employ security standards including TLS 1.2 Transport Level Security protocol, SFTP protocol for managed file transfers, and certificate authentication for file transfer portals. AES 256-bit encryption, together with these protocols, meets the secure standards required for exchange of PHI under HIPAA and HITECH.

FDGS gives highest priority to protecting the security and privacy of DHHR data, and especially the security of the environment that houses it. Your EVV vendor has a critical role in maintaining overall compliance with security and privacy laws, regulations, and CMS standards. The AuthentiCare platform provides world-class security thanks to our global security practices and procedures. Fiserv processes $4 trillion in banking and credit card transactions annually and has a record for proactive security and privacy protection.

Table 7.9 – AuthentiCare Meets all Mandatory Requirements for Security Management

Met	Req ID #	Requirement Text
☑	**MR013**	The solution must uniquely identify each user.
☑	**MR016**	The Vendor must establish business associate agreements (BAA) or contractual agreements with the Department and any subcontractors according to Federal agency requirements that have access to data which is subject to protection by the Health Insurance Portability and Accountability Act (HIPAA). (Reference: https://www.hhs.gov/hipaa/index.html)
☑	**MR017**	The Vendor must agree to enter into applicable Business Associate Agreements (BAA) with external electronic visit verification (EVV) data partners as directed by the Department prior to accepting or exchanging protected health information (PHI) and/or personally identifiable information (PII) data from the EVV solution.

☑	**MR018**	The Vendor must ensure that all data submitted to or collected by the solution will remain the property of the Department.
☑	**MR019**	The Vendor must agree to abide by all the Department security and privacy policies to protect confidential and sensitive information.
☑	**MR020**	The solution must have the ability to receive, store, and exchange protected health information (PHI) and personally identifiable information (PII) through authentication, along with encryption methods to secure sensitive information following nationally recognized standards, including the privacy and security controls outlined within National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations special publication (SP) 800-53 (moderate) and NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices. (Reference: https://csrc.nist.gov/publications/detail/sp/800-111/final and https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)
☑	**MR021**	The solution must use only Federal Information Processing Standard (FIPS) Pub 140-2 validated (or higher) encryption or equivalent. (Reference: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf, and https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf)

To provide effective security management, AuthentiCare leverages the comprehensive corporate policy approach based on a robust Global Cyber Security and Fraud Policy. Our Cybersecurity and the General Counsel Office consist of various domestic teams, each specializing in a different aspect of IT security, risk, compliance, and audit, with a total U.S. staffing greater than 300, most of whom have more than 12 years of IT security experience and multiple certifications covering technology, security, privacy, legal, audit, and safety.

These teams are responsible for creating and maintaining security policies and standards, risk management, investigations and threat management; overseeing their implementation; and validating compliance. The Information Security Policy framework is based on multiple International Standards Organization (ISO) 27001 standards and is fully complementary to the ISO-2013 cyber security controls. We have chosen this broader approach rather than the strict adherence to one standard because it enables a single, global Fiserv IT security policy that meets the full scope of legal and regulatory requirements across a diverse spectrum of products and services. All Fiserv employees, including our proposed team, meet or exceed mandatory security compliance requirements.

FDGS provides additional detail to the Security Management Subject Matter Area requirements in Table 7.10.

Table 7.10 – Detailed Response to Security Management Requirements

Req. ID #	Requirement Text	Requirement Type
SM001	The solution should authenticate all users when establishing a connection to the solution.	Security Management
All AuthentiCare users must provide their unique credentials at the time of log in. Each user is assigned a role with the appropriate responsibilities for their role so they are provided the appropriate level of access and no more. AuthentiCare's solution for role-based permissions is compliant with NIST guidance for identification, authentication, and authorization. The AuthentiCare mobile and IVR options both employ two-factor authentication preventing unauthorized access.		
SM002	The solution should have the ability to automatically generate a unique user identification during the registration process for new users enrolling in the program.	Security Management
AuthentiCare automatically generates and assigns a unique user ID during the onboarding process. Each AuthentiCare user of the web portal and mobile app is granted specific role-based access through the use of this unique user ID.		
SM003	The solution should have the ability to assign a new unique user identifier (ID) for an existing user.	Security Management

Req. ID #	Requirement Text	Requirement Type
If, for some reason, an existing user requires a new unique user ID, their prior user record will be made inactive and the existing user will need to be registered to AuthentiCare to get a new user ID.		
SM004	The solution should use a secure file transfer protocol (i.e. SFTP, etc.), secure web interface, or other industry-standard electronic means (such as Gentran, Connect: Direct, or equivalent) or encrypted media to transfer files as approved by the Department.	Security Management
AuthentiCare EVV processes employ Security Standards including TLS 1.1 or 1.2 Transport Level Security protocol, SFTP protocol for managed file transfers through the FDGS File Gateway, and certificate authentication for file transfer portals. AES 256-bit encryption, together with these protocols, meets the secure standards required for exchange of PHI under HIPAA.		
SM005	The solution should warn the user about accessing US Government Federally protected data and allow the user to confirm and proceed with such actions.	Security Management
AuthentiCare will present a warning message regarding access to US Government Federally protected data. DHHR will provide the prescribed warning message text.		
SM006	The Vendor should provide a secure web-based method to receive requests for authorization to access the solution.	Security Management
AuthentiCare's solution for role-based permissions is compliant with NIST guidance for identification, authentication, and authorization. New users are added to AuthentiCare using our secure, web-based application.		
SM007	The Vendor should provide Single Sign-On (SSO) capability for authentication and authorization across the solution.	Security Management
AuthentiCare provides a single sign-on across its EVV web portal.		
SM008	The solution should provide Department-approved multi-factor authentication for Vendor remote access to solution environment or their contractors, if applicable.	Security Management
AuthentiCare's web, mobile, and IVR modules employ two-factor authentication preventing unauthorized access to the application, visit data, and any mobile device. Access to AuthentiCare environments is carefully restricted to only necessary staff. Staff must individually authenticate to each server with a public/private key pair in order to access AuthentiCare environments. In addition to user name and strong password, the AuthentiCare web will use a time-sensitive, one-time PIN, while the mobile app will use user name and password along with the device ID.		
SM009	The solution should use role-based access for data and system functionality.	Security Management
At the EVV application level, the AuthentiCare solution is configurable for any number of roles and rights combinations. However, in our experience, most of the default provider roles and their accompanying rights are sufficient for most implementations. These standard roles were defined with the assistance of providers and state staff in other states. We can easily configure the roles based on input from providers and staff in West Virginia. The "Super User" role will be validated with all appropriate access during the Design Sessions. AuthentiCare's solution for role-based permissions is compliant with NIST guidance for identification, authentication, and authorization. FDGS will work with the Department to set the appropriate access to all features and functions based on the user role. For example, a "Scheduler Coordinator" role could be limited to specific scheduling functions and reports related to scheduling like the Calendar and Late and Missed Visits Reports. Another scenario within our AuthentiCare solution allows all web users to set report content and run reports in real-time or on a schedule, but only reports and content for which their user role gives access. FDGS will work with the Department to establish role-based access to the reporting function. As an example, a common standard provider role is the "Administrator" or "Admin Assistant," which has access to all reports. Other standard roles like "Human Resources'" would be limited to worker-related reports. This information will be included in the AuthentiCare Reporting User Guide. As DHHR continues to use AuthentiCare and determines changes to the roles and access are necessary, FDGS will support the Department with the appropriate configuration updates. AuthentiCare allows DHHR staff to simply configure system changes on their own to adjust roles and access as policies and procedures are updated. Details for user roles and access to the AuthentiCare functions are documented in the AuthentiCare User Guide for easy reference.		
SM010	The solution should have configurable roles by state plan and waiver program that may be created and modified by the Department through a	Security Management

Req. ID #	Requirement Text	Requirement Type
	change request as outlined in the Department approved Change Management Plan.	
FDGS agrees to support the configuration of additional roles for state plan or waiver programs that may be created and modified by the Department through a change request as outlined in the Department approved Change Management Plan.		
SM011	The solution should have the ability to record specific access by users to confidential personal information (CPI) contained within the solution. The mechanism should record the following data elements and allow a role-based user to search this log for matching criteria to discern what was accessed including, but not limited to:	Security Management
SM012	User name	Security Management
SM013	Date of access	Security Management
SM014	Time of access	Security Management
SM015	Name of Individual (First and Last) whose confidential personal information (CPI) was accessed	Security Management
SM016	Name of computer system used to access confidential personal information (CPI)	Security Management
SM017	Query/Transaction used	Security Management
AuthentiCare will record specific access to CPI data. To support CMS certification, AuthentiCare will record user name, date and time of access, and the name related to the CPI accessed. Access to all CPI is managed through the user roles defined by the Department and the access granted once the user logs in with their secure credentials. AuthentiCare also records specific modifications to CPI (and other system data) as part of our standard audit process. The AuthentiCare solution does not record the computer system name or the query/transaction used to access CPI. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
SM018	The solution should provide users role-based access to reporting functionality.	Security Management
AuthentiCare's role-based access is integrated across all EVV system components including the reporting engine. Only data that is appropriate by role is available through the reporting functionality. FDGS will work with the Department to finalize role-based access to the reporting function. As an example, a common standard provider role is the "Administrator" or "Admin Assistant," which has access to all reports. Other standard roles like "Human Resources'" would be limited to worker-related reports. These final role-based access definitions will be included in the AuthentiCare Reporting User Guide.		
SM019	The solution should allow correspondence to be viewed based on role based access.	Security Management
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
SM020	The solution should allow authorized users to remove view or edit access rights to any data fields or data elements within the solution based on user role.	Security Management
AuthentiCare's security solution uses role-based authorization to provide access to system-level components including access to individual windows, pages, or reports. In general, page design incorporates the data elements and fields included and authorized access to an entire page allows or prevents these data elements to be viewed. FDGS will work with the Department to define the roles appropriately and can share the data that is configurable from a viewing/editing standpoint.		

Req. ID #	Requirement Text	Requirement Type
SM021	The solution should provide role-based security through various methods, including, but not limited to:	Security Management
SM022	Unique identifiers (IDs)	Security Management
SM023	Mandatory password standards and policies for length, character requirements, and updates for all users as defined within National Institute of Standards and Technology (NIST) 800-63-3: Digital Identity Guidelines, or equivalent. https://doi.org/10.6028/NIST.SP.800-63-3	Security Management
SM024	Profile or group access assignments	Security Management
Each AuthentiCare user of the web portal and mobile app is granted specific role-based access through the use of a unique user ID. Our minimum password policies can be configured to even higher standards at the Department's request. Password requirements include length, strength, complexity, change frequency, and history. AuthentiCare's role-based security supports a hierarchical structure in which users are granted access to specific areas, functions, and data within the product. Users are assigned to roles that are granted specific rights to access within the system.		
SM025	The solution should provide a mechanism to limit access to information based on user roles and program rules.	Security Management
In addition to AuthentiCare's role-based access, our solution supports the use of additional business rules at the program level to further limit access according to Department policies.		
SM026	The solution should provide role-based access to all system components and control access through various methods, including, but not limited to:	Security Management
SM027	Blocking specific window or screen access	Security Management
SM028	Blocking specific report views or analytics	Security Management
SM029	Restrict data elements	Security Management
SM030	Restrict viewing of specific members	Security Management
SM031	Limit access to other fields within the system as determined by the Department	Security Management
AuthentiCare's security solution uses role-based authorization to control access to system-level components including access to individual window, report, data element, and field levels.		
SM032	The solution should update all security roles automatically when a change in the master role is made.	Security Management
Role-based access is effective immediately once the access rule configurations are saved for each user role.		
SM033	The solution should allow user access and role changes to be made in real-time.	Security Management
Role-based access is effective immediately once the access rule configurations are saved for each user role.		
SM034	The solution should have the ability to restrict concurrent logons.	Security Management
AuthentiCare supports the ability to restrict concurrent logons.		
SM035	The solution should have the ability to configure the timeout requirements for each system environment and user role.	Security Management
AuthentiCare includes configuration attributes to modify the timeout requirements within each system environment and user role. The values will be verified during the requirements validation and Design Sessions.		
SM036	The solution should have the ability to create multi-level escalating alerts for Department-defined events.	Security Management
AuthentiCare is easily configurable to set up multi-level escalating alerts for late or missed visits and other Department-defined alerts. AuthentiCare delivers the ability to configure automated alerts, such as when services are late or		

Req. ID #	Requirement Text	Requirement Type
missed, so a qualified back-up worker may be dispatched. Automated alerts may be sent via email to designated recipients as determined by Department policy. Support coordinators, provider agencies, emergency back-up workers, or state staff may be notified that a critical service has not been delivered. Alerts may also be configured to meet the requirements of individual services or programs as the Department chooses, and alerts can go to multiple recipients as defined in the template. These alerts can be tracked by caregiver, by provider, or by recipient in various reports and dashboards to identify trends that need to be addressed. To prevent "alert fatigue," it is critical to define timing and escalation of the alerts to maximize the meaning of an alert when it is received, and minimize the number of false alarms. AuthentiCare alert thresholds can use statewide default values or specific values for a type of service. Optionally, there can be special values for specific critical recipient needs, like for at-risk recipients. Alerts can be disabled for some services (for example, services that are not scheduled, or unit-based services like Home Delivered Meals), or for situations where the recipient is in a remote "no tech zone" where the visit data will be submitted by Store and Forward from the Mobile App at a later time. These options reduce false alarms. Automated alerts are sent via email to designated recipients. Support coordinators, provider agencies, emergency back-up workers, or State staff may be registered to be notified that a critical service has not been delivered. For example, AuthentiCare can be configured so that only Providers receive late alerts whereas care managers, state staff, or others could be notified of missed alerts only.		
SM037	The solution should identify the recipients of alerts by alert type and user role.	Security Management
For each alert type, the AuthentiCare configuration rules identify the appropriate recipient(s) by user role.		
SM038	The solution should have the ability to allow the Department to define which edits and rules may be overridden within the solution by the direct care worker or provider agency and how the solution will respond with warnings, alerts, or denials of the requested user action.	Security Management
The AuthentiCare solution uses a table-driven rules approach, which supports easy additions to services and updates to business rules as services and waiver rules change, to configure EVV services. Business rules may result in warnings, alerts, or denials of a requested action. FDGS will work with the Department to define when a rule results in a warning that allows the DCW or user to continue through the warning. Other business rules and edits will be defined to prevent users from continuing without addressing the rule/edit conflict. Within the standard rule set supported by AuthentiCare, rules can be added, updated, or changed by changing table entries. The rules for DHHR are documented in a tabular format in the AuthentiCare System Integration Plan (SIP).		
SM039	The solution should utilize a Security Information and Event Management (SIEM) solution that generates alerts for events. Copies will be made available to the Department, including, but not limited to:	Security Management
SM040	Alert generation for attempts to access unauthorized databases from internal and external systems	Security Management
SM041	Monitoring and reporting of events on an ongoing basis	Security Management
Log data are collected in a central logging platform and fed into Fiserv's Security Operations Center (SOC) toolset for monitoring and alerting, which is staffed 24x7. Review of audit logs are configured through Splunk to meet these monitoring requirements for unauthorized access and ongoing reporting of events. AuthentiCare logs errors using a variety of software tools and technical processes. The data captured includes extensive data specific to each error. Generally, our technical analysts use licensed software to further research errors and determine root cause. The raw log data are not normally shared with customers to prevent release of confidential data and its proprietary format. Splunk is used as a central repository for log data. Cyber security incidents may be detected through many different means, automated and manual, all with varying level of details and fidelity. Several of the most common sources of events are automated alerts from log sources, Fiserv/FDGS owner associates, and intelligence sources. CSIRT is responsible for the process of receiving, triaging, and handling alerts. Our firewall team performs semiannual reviews of firewall rules considered to be of the most risk to the organization. This review is documented by location and firewall type. Changes made to the firewalls go through the infrastructure change procedures. Fiserv also uses multiple tools for monitoring various aspects of the firewalls. Tufin is used to track changes to firewall rules. Any past rule configurations are available for review. A specific username and various other details are collected for firewall rule changes. All of these tools contribute to the monitoring of the firewall setups.		
SM042	The Vendor should provide a report outlining applicable National Institute of Standards and Technology (NIST) SP 800-53 moderate security control	Security Management

Req. ID #	Requirement Text	Requirement Type
	responsibilities (reference: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) noting which security controls are implemented and/or inherited by the Vendor, implemented by the Department, or shared by both parties. This report should be maintained by the Vendor and outline the following information, including, but not limited to:	
SM043	Non-compliant and required security and privacy controls	Security Management
SM044	Applied mitigations	Security Management
SM045	Plan to correct deficiencies	Security Management

FDGS hosts AuthentiCare in our captive cloud virtualized environment that adheres to the NIST CSF and NIST 800-53 moderate baseline at a minimum. FDGS agrees to provide a report documenting the adherence with EVV-applicable NIST standards and guidelines.

Our IT policies are based on multiple industry standards for security and privacy. FDGS will provide the following items as part of Standards Compliance:

1. HIPAA
2. NIST 800-30 r1
3. NIST 800-37
4. NIST 800-53 r4
5. FIPS 140-2
6. PCI-DSS
7. SOC 1/SSAE-18
8. GLBA
9. FISMA
10. CCPA (California Consumer Privacy Act)
11. GLBA (Gramm-Leach-Bliley Act)
12. NYDFS Cyber security regulations

It is this level of protection that protects all of our applications and financial transactions; satisfying the highest level of audit and regulatory scrutiny. Please note that some reports will require a Non-Disclosure Agreement (NDA) prior to release outside of FDGS.

SM046	The solution should maintain a list of users and owners of each stored report.	Security Management

AuthentiCare does not store reports in the same way that legacy applications may have. Instead, the main reports engine web page provides authorized, but easy, access to run on-demand reports, as well as create and schedule regular reports for re-use, and then pick up completed reports in the user's preferred format (including PDF, Excel, and XML). The system allows the user to schedule or submit report requests, do other work while the reports run, and then come back to the page to pick up their reports when they are ready.

SM047	The solution should retain and maintain access to reports as specified by the Department's Retention Policy. (Reference: https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2019/PO1013_DataBackup_Mar2019.pdf)	Security Management

FDGS has reviewed the Department's Backup and Retention Policy. The AuthentiCare solution supports the retention and maintenance of access to reports and supporting data according to the policy. AuthentiCare's default for backup and archiving of EVV data is seven years.

SM048	The solution should allow, initially, up to fifteen (15) State users to create ad hoc reports. Additional users should be added at no additional cost to the State.	Security Management

There is no limit to the number of users that can use AuthentiCare's reporting module. The number of users is only dependent on the number that the Department authorizes to be in those roles.

The AuthentiCare solution includes a robust reporting engine for use in EVV program monitoring and management, and to help identify and reduce fraud, waste, and abuse. AuthentiCare contains a broad spectrum of on-demand reports that contain ad hoc functions like drop down list filters, parameters, date ranges, and other selections that allow users to report the data of which they are specifically interested.

Req. ID #	Requirement Text	Requirement Type
This allows the Department and providers the ability to search through summary and detailed data views. Using selection criteria for each report, a user can customize the standard report to meet specific requirements easily and simply, and run a one-time report, or save a report that they want to run regularly for ongoing analysis or metrics submissions. These reports provide stakeholders, as well as the provider community (based on their security access authority), views into the electronic visit and verification data to manage the programs, confirm beneficiaries receive needed care, and help identify fraud, waste, and abuse.		
SM049	The solution should track and store detailed information regarding all reporting requests, including, but not limited to:	Security Management
SM050	Who requested the information	Security Management
SM051	Date of request	Security Management
SM052	Time of request	Security Management
SM053	What data the report included	Security Management
SM054	Report storage upon completion	Security Management
AuthentiCare does not store reports in the same way that legacy applications may have. Because of the way reports are requested and executed, AuthentiCare is able to meet each of the tracking and storage of the related report metadata including requester, date and time, report data, and storage details. (see also SM046)		
SM055	The solution should generate a periodic report of upcoming user account terminations on a schedule approved by the Department	Security Management
AuthentiCare does not currently support the periodic reporting of upcoming user account terminations. Administrators are able to go directly into AuthentiCare as account terminations are needed. AuthentiCare does maintain data within the system to identify those user accounts that will be automatically disabled due to inactivity for a configurable amount of time. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
SM056	The solution should maintain a record of all Integrated Eligibility Solution (IES) member information accessed.	Security Management
AuthentiCare will record specific access to Integrated Eligibility Solution (IES) member information. To support CMS certification, AuthentiCare will record user name, date and time of access, and the name related to the IES member accessed. Access to all IES member information is managed through the user roles defined by the Department and the access granted once the user logs in with their secure credentials. AuthentiCare also records specific modifications to Integrated Eligibility Solution (IES) member information (and other system data) as part of our standard audit process.		
SM057	The solution should maintain a record, including an audit trail, of all manually entered data queries by user, communications, and report distributions.	Security Management
AuthentiCare does not currently record all data queries by our support staff, including DBAs. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
SM058	The Vendor should supply, on an annual basis, a report of the results of all security, privacy, and risk assessments, including all tools used, and an action plan detailing the approach for remediation of security risk vulnerabilities. Data and testing results, including reports, should be retained for 10 years per CMS guidelines.	Security Management
FDGS agrees to provide an annual summary report of our security, privacy, and risk assessments. We will work with the Department to maintain the report location and retention according to CMS guidelines. Internal Audit performs an annual risk assessment to establish the upcoming year's Audit Plan. Internal Audit		

Req. ID #	Requirement Text	Requirement Type
continuously reviews business processes to help confirm that the audit universe is complete. Each auditable entity is risk rated as High, Moderate, or Low considering its size, scale, and complexity, as well as operational, financial, compliance, technology, and fraud risks. During the audit plan year, Internal Audit holds formalized sessions to update risk ratings based on its monitoring activities. This helps verify that the audit plan is adequately refreshed in response to any significant changes in risk across Fiserv. The Audit Plan calls for auditable entities rated High to be audited annually, those rated Moderate to be audited no less than every two years, and those rated Low to be audited no less than every three years. Risk ratings are refreshed throughout the year based on continuous internal monitoring procedures. The Audit Plan and risk ratings are shared with Fiserv management, and comments are considered to finalize the Audit Plan. The final Audit Plan is approved by Fiserv's Audit Committee, and any subsequent changes are approved by the Internal Audit Leadership Team and reported to the Audit Committee. Internal Audit performs a risk assessment of each auditable entity to identify key objectives and risks, which will serve as the baseline for the entity's audit program. This will include financial, operational, compliance, technology, and fraud risks. Internal Audit meets with process owners to identify the controls implemented by management to mitigate these risks. Internal Audit reports findings, control gaps, process improvements, and/or observations to management after the completion of fieldwork. Each audit report is assigned an overall rating of Satisfactory, Needs Improvement, or Unsatisfactory based on the level of assurance Internal Audit can place on the entity's control environment. Internal Audit tracks management's remediation of each identified issue. Upon completion, Internal Audit performs risk-based validation procedures to assess the effectiveness of the remediation effort. Internal Audit routinely presents to the Audit Committee and senior management the following information: audit reports rated as Needs Improvement or Unsatisfactory, findings with remediation efforts that failed, findings with remediation efforts that are past due, findings that were risk accepted by Fiserv management, and newly issued high rated findings.		
SM059	The solution should log manual overrides and report on them at timed intervals determined by the Department.	Security Management
Manually entered edits, corrections, and overrides are performed in an AuthentiCare web process where specific authorized users can make corrections, and, for some types of edits, specific users are empowered to approve or deny them before billing can take place. AuthentiCare supports requiring a reason code for reporting and visit note for added or edited services. The system also provides a full audit trail of changes made including date, time, user ID, and a record of the change. AuthentiCare supports the ability for a provider to add notes and text explanations. The Claim History Report can be run at any time, and includes details of edits and changes and supports viewing of notes added to each record.		
SM060	The solution should create a log of access attempts and generate a monthly user lock out report to the Vendor's security management team and to the Department, upon request.	Security Management
AuthentiCare tracks access attempts and lockouts, but does not currently generate a report of user lockouts. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
SM061	The solution should have the ability to provide authorized requestors a report containing the security profile for an individual or role.	Security Management
AuthentiCare provides screen views to see security profiles for an individual or role. AuthentiCare does not currently generate a report containing security profiles by individual or role. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
SM062	The solution should monitor, detect, and report impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.	Security Management
AuthentiCare does not currently monitor, detect, or report impermissible use. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
SM063	The Vendor should conduct annual penetration testing of the solution and provide results to the Department within 30 days of completion.	Security Management

Req. ID #	Requirement Text	Requirement Type
Fiserv's Unified Vulnerability Management Services (UVMS) Team's primary responsibility is to perform annual penetration tests and vulnerability assessments of Fiserv's infrastructure and applications. UVMS also performs semiannual segmentation tests as required by PCI. UVMS plays a vital role in helping to protect customer information and Fiserv's assets. Upon award, FDGS will provide the date of the most recent test cycle. FDGS agrees to provide results within 30 days of the annual test report availability. The penetration testing process used is a 'gray' box approach as defined in NIST 800-115 Technical Guide to Information Security Testing and Assessment. Penetration tests are designed to be non-destructive, and minimize the potential impact to systems or networks under test. Fiserv facilitates an annual third-party security assessment of external networks. These tests are performed in addition to UVMS testing, and are executed by an approved, independent third party. Vulnerabilities deemed of risk to Fiserv are assigned to appropriate individuals who are required to take action to mitigate any risks associated with identified vulnerabilities. Prior to implementation, Fiserv will verify with the Department the date since the completion of the most recent penetration and vulnerability tests. An attestation to test results will be shared with the Department. The remediation plan and timeframes will be available to the customer for viewing onsite, pursuant to relevant product and network results. Due to the breadth of the Fiserv environment and the level of confidential and proprietary information that may be included in test results, information relevant to the client's data and contract requirements may be shared in a controlled environment.		
SM064	The Vendor should provide all incident reporting to the Department immediately upon discovery per Department guidelines	Security Management
In the event that FDGS/Fiserv becomes aware of an actual loss or unauthorized use, disclosure, alteration, destruction, or other compromise or unauthorized acquisition of or access to any Personal Information in Vendor's possession (an "Information Security Incident"), FDGS will: (a) assess the nature and scope of the Information Security Incident; (b) promptly take appropriate steps to contain and control the Information Security Incident to prevent further unauthorized access to or misuse of the information; (c) promptly conduct a reasonable investigation to identify what systems and types of information have been accessed and to determine the likelihood that the information has been or could likely be misused; (d) *promptly notify the Department of the material details of the Information Security Incident that are known at the time of notification, subject to a request by law enforcement or other government agency to withhold such notice*; and (e) continue to provide information relating to the investigation and resolution of the Information Security Incident until FDGS/Fiserv reasonably determines the Information Security Incident has been resolved. As part of our Incident Management method, our Cyber Security Incident Response Team (CSIRT) is a Global Cyber Security and Fraud initiative designed to provide a systematic response facility to cyber security incidents. The CSIRT program mission is to minimize the impact of incidents by executing a rapid and consistent response, gathering and disseminating information to better prepare for future cyber security incidents, and improving awareness and knowledge of cyber security threats impacting Fiserv and our customers.		
SM065	The solution should be able to redact information contained in any form, correspondence, or report and save the redacted version as a new file.	Security Management
AuthentiCare reports only include data that are authorized by the requester's role. AuthentiCare does not currently support automated generation of forms or correspondence, including redaction of information within a form, correspondence, or report. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
SM066	The solution should allow users to override and change pre-populated information in forms, when appropriate.	Security Management
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
SM067	The solution should maintain an inventory and store all system-generated correspondence based on Bureau for Medical Services' (BMS) Retention Policy (Reference: https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2019/PO1013_DataBackup_Mar2019.pdf)	Security Management
AuthentiCare does not currently support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work		

Req. ID #	Requirement Text	Requirement Type
with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
SM068	The solution should ensure that data, including hard copy documents, are retained, stored, imaged, archived, and protected from destruction. All data should be available according to Department and federal requirements, and in accordance with the Department's Data Retention Policy (Reference: https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2019/PO1013_DataBackup_Mar2019.pdf)	Security Management
AuthentiCare data are stored, replicated, and backed-up in accordance with the Department's Data Retention Policy.		
SM069	The Vendor should ensure that hard copy documents are retained, stored, imaged, archived, and destroyed in accordance with applicable federal requirements and in accordance with the Department's Data Retention Policy (Reference: https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2019/PO1013_DataBackup_Mar2019.pdf)	Security Management
If hard copy documents are uploaded to AuthentiCare, storage, retention, and back-ups will follow the Department's Data Retention Policy.		
SM070	The solution should prevent certain decisions and fields from having the ability to be overridden by users.	Security Management
All data fields and decisions within AuthentiCare are configurable to prevent an override by users.		
SM071	The Vendor should ensure that information captured via the web portal meets the relevant data management specifications, including, but not limited to, access, inquiry, update, retention, and archival.	Security Management
All information captured via the AuthentiCare web portal is validated by our quality assurance processes to meet the relevant data management specifications, including, but not limited to, access, inquiry, and update. The AuthentiCare system architecture resides in our primary and secondary data centers to provide automated data replication, storage, retention, and archival according to the data management specifications.		
SM072	The solution should have the ability to display and require the user to accept web-site terms of agreement when entering the web portal.	Security Management
AuthentiCare will display website terms of agreement when entering the web portal. The user will be required to accept the agreement before they will be allowed to continue.		
SM073	The solution should have the ability to establish user access to predefined Department levels including, but not limited to:	Security Management
SM074	Page level	Security Management
SM075	Field level	Security Management
SM076	Data element level	Security Management
AuthentiCare supports predefined user-limited access at the page, field, and data element level through the definition of specific user roles approved by the Department. All user role definitions will be validated during the iterative design and configuration sessions. FDGS will work with the Department to set the appropriate access to all features and functions based on the user role. For example, a "Scheduler Coordinator" role could be limited to specific scheduling functions, pages, and reports related to scheduling like the Calendar and Late and Missed Visits Reports. Another scenario within our AuthentiCare solution allows all web users to set report content and run reports in real time or on a schedule, but only reports and content for which their user role gives access.		
SM077	The Vendor should provide a public facing website that provides access to a secure portal including, but not limited to:	Security Management
SM078	Instructions on how to use the secure site	Security Management
SM079	Site map	Security Management

Req. ID #	Requirement Text	Requirement Type
SM080	Contact information	Security Management
FDGS will provide a public-facing website that includes access to the secure portal. Once the user logs in, they will have access to instructions, a standard site map, and contact information as agreed to by the Department. The AuthentiCare landing page also includes information to contact the AuthentiCare help desk and access to all of the on-demand training content.		
SM081	The solution should have the ability to send users their initial auto-generated password via email and require that they change their password upon their next sign-on.	Security Management
The initial password must meet minimum password complexity standards. Initial passwords are set by the administrator creating the user account and communicated by the administrator to the user. Passwords expire after a configurable period. If a user password expires, the user is required to change the password upon their next sign-on. AuthentiCare does not currently support automated generation of passwords nor email notifications for new passwords. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
SM082	The solution should have the ability to require qualifying information to access system records via the web portal including, but not limited to:	Security Management
SM083	Provider number	Security Management
SM084	Prior authorization number	Security Management
SM085	Medicaid ID number	Security Management
SM086	Date of service	Security Management
SM087	Claim number	Security Management
As part of the built-in navigation within the AuthentiCare web application, additional qualifying information may be required for appropriate access including Provider number, Prior authorization number, Medicaid ID number, Date of service, or Claim number. These and other data element keys must be provided to access lower-level details related to each key.		
SM088	The solution should allow a system administrator to reset user passwords.	Security Management
AuthentiCare allows a system administrator to reset user passwords.		
SM089	The solution should allow users to change their passwords on demand.	Security Management
AuthentiCare allows individual users to maintain their own passwords on demand.		
SM090	The solution should have the ability to set and adjust password expiration dates.	Security Management
AuthentiCare provides a configurable time period for password expiration. For example, passwords may be allowed to remain current for 120 days during the initial startup period, but once the system is accepted and is stable, the password expiration could then be easily updated to a 60-day expiration period.		
SM091	The solution should have the ability to warn the user that the Caps Lock is on when entering sign-on passwords.	Security Management
AuthentiCare web and mobile applications only use device-specific notifications to warn the user that Caps Lock is on when entering sign-on passwords. AuthentiCare does not currently support warnings when Caps Lock is on. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
SM092	The Vendor should establish an expiration schedule for system component required passwords to minimize system or user disruption.	Security Management

Req. ID #	Requirement Text	Requirement Type
AuthentiCare provides a configurable time period for password expiration. For example, passwords may be allowed to remain current for 120 days during the initial startup period, but once the system is accepted and is stable, the password expiration could then be easily updated to a 60-day expiration period. Our data center support staff also follow strict password requirements and expiration schedule to maintain the highest security levels and avoid system or user disruption.		
SM093	The solution should store passwords in encrypted form. The Advanced Encryption Standard (AES) 256-bit standard or equivalent should be used. (Reference: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf)	Security Management
AuthentiCare web application passwords are encrypted in the database using an encrypted hash with random salt to meet the equivalent requirement. Mobile passwords are stored in the AuthentiCare portal and compared as SHA 512-bit encrypted hash, so that only the mobile user knows the pass phrase used to generate the hash.		
SM094	The solution should enforce password policies for length, character requirements, and updates for all users as agreed upon by the Department	Security Management
Our minimum password policies can be configured to even higher standards at the Department's request. Password requirements include length, strength, complexity, change frequency, and history.		
SM095	The solution should allow self-service password resets.	Security Management
AuthentiCare will support self-service password resets. Administrators and the AuthentiCare help desk also support password resets.		
SM096	The solution should send system-generated email notifications of password change events and expiration warnings at Department approved intervals.	Security Management
AuthentiCare does not currently support system-generated email notifications of password change events and expiration warnings. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
SM097	The Vendor should deactivate all system access for users immediately upon notification of termination, departure, or reassignment.	Security Management
AuthentiCare supports the immediate deactivation of user access by administrators or the AuthentiCare help desk once notified by the Department. If users move to a new role, their access will be appropriately modified to the new user role based on their new position and access requirements.		
SM098	The solution should have the ability to lock out a user after a pre-determined number of unsuccessful login attempts.	Security Management
AuthentiCare provides a configurable setting to define the number of unsuccessful login attempts allowed before a user is locked out.		
SM099	The solution should automatically suspend all users who have not accessed the solution within a specified period of time as requested by the Department.	Security Management
AuthentiCare provides a configurable setting to define the period of time allowed before a user's access is automatically suspended. Either an administrator or the AuthentiCare help desk will reactivate the user before they can access AuthentiCare again.		
SM100	The solution should have the ability to close accounts that have been suspended more than a predetermined number of days as requested by the Department.	Security Management
AuthentiCare provides a configurable setting to define the period of time before a suspended account is inactivated or closed due to inactivity.		
SM101	The solution should have the ability to terminate authorized sessions after predetermined time period of inactivity, as requested by the Department, after a warning message is displayed to the user informing them that the session will terminate in an identified period of time.	Security Management
AuthentiCare provides a configurable setting to define the period of time allowed before a user's authorized access is terminated due to inactivity. The web application provides a warning message at a pre-set time prior to the session termination so that the user may continue and avoid losing any unsaved work prior to the automated session termination.		
SM102	The solution should provide three types of controls to maintain the integrity, availability, and confidentiality of protected health information (PHI) data contained within the system. These controls should be in place at all	Security Management

Req. ID #	Requirement Text	Requirement Type
	appropriate points of processing as follows:	
SM103	Preventive Controls: Controls designed to prevent errors and unauthorized events from occurring	Security Management
SM104	Detective Controls: Controls designed to identify errors and unauthorized transactions that have occurred in the system.	Security Management
SM105	Corrective Controls: Controls designed to ensure that the problems identified by the detective controls are corrected.	Security Management

Fiserv/FDGS provides several controls to maintain the integrity, availability, and confidentiality of PHI/PII and other confidential data within AuthentiCare and our other systems. Our Defense in Depth security model (presented in Figure 7.12) provides an extensive system of physical, technical, and administrative controls to protect EVV data through:

- System access security
- Network security
- Application design and security
- Physical access security
- Data security and encryption

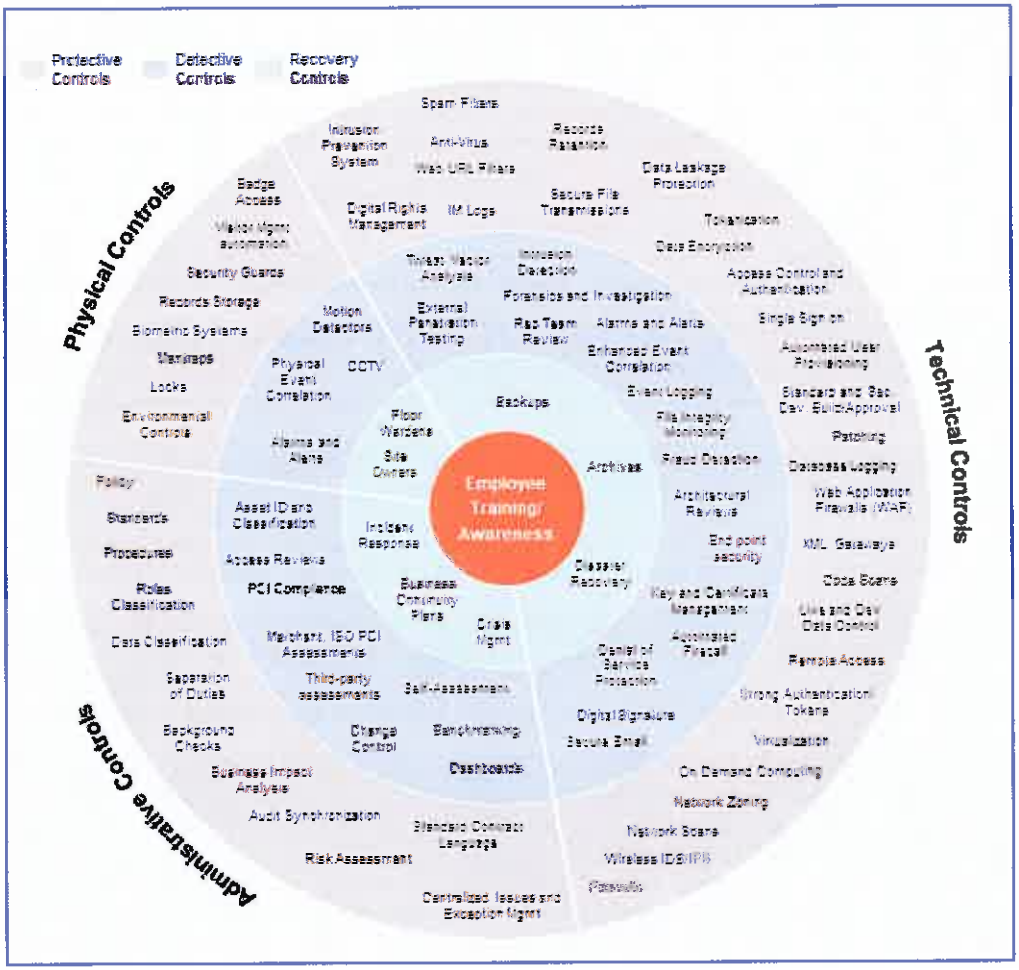


Figure 7.12 – AuthentiCare provides Preventive, Detective, and Corrective controls within our extensive Defense in Depth model of system security

Req. ID #	Requirement Text	Requirement Type
	Preventive Controls (Protective): In addition to monitoring network connections and incoming traffic, Fiserv also maintains and monitors a Data Loss Prevention (DLP) system to prevent egress of network data and email traffic containing PHI/PII. This additional check on outgoing flow of specific types of data offers extra protection by preventing specific data from leaving our secure environment. **Detective Controls:** Intrusion Detection is in place on the following segments: Internet point-of-presence, DMZ, extranet, internal production network, and network segment hosting target data. It is configured to generate alerts in case of incidents and values exceeding normal thresholds for the environment. A formal process is in place to regularly update the Intrusion Detection System (IDS) signatures based on new threats and changes in the environment. The system is electronically monitored 24x7x365. IDS events feed into the Incident Management process that alerts operations personnel to take action to resolve the issue. **Corrective Controls (Recovery):** Corrective measures will be taken to repair damage or restore resources and capabilities to their prior state following an unauthorized or unwanted activity. Examples of technical corrective controls include patching a system, quarantining a virus, terminating a process, or rebooting a system. For significant recovery, system backups and archives are available to execute the approved Disaster Recovery/Business Continuity plans.	
SM106	Upon login, the solution should inform users of privacy policy, including the logging of users' access attempts to personally identifiable information (PII) and/or protected health information (PHI) and other actions taken within the application that are subject to privacy reporting and disclosure notification, including the legal sanctions imposed for improper disclosure and use to be approved by the Department	Security Management
Once logged in, the user is presented the AuthentiCare landing page. FDGS will work with the Department to finalize the language to include informing the users of privacy policy, including the logging of users' access attempts to personally identifiable information (PII) and/or protected health information (PHI) and other actions taken within the application that are subject to privacy reporting and disclosure notification, including the legal sanctions imposed for improper disclosure and use. The layout and format of the privacy policy language will also be finalized during the design and configuration sessions.		
SM107	The Vendor should deliver reporting on all unauthorized disclosures of personally identifiable information (PII) and/or protected health information (PHI) immediately upon discovery.	Security Management
If unauthorized disclosures of personally identifiable information (PII) and/or protected health information (PHI) are discovered, FDGS agrees to promptly report available details to a designated recipient within the Department; provided, however, that our ability to report to you is not subject to any request by law enforcement or other government agency to withhold such notice.		
SM108	The Vendor should perform data mapping to identify confidential data and Protected Health Information (PHI) contained in the system, the flow of that data through the system, and where that data resides.	Security Management
FDGS agrees to work with the Department throughout the iterative design and configuration sessions to verify the identification, flow, and storage of confidential data and Protected Health Information (PHI) contained within AuthentiCare.		
SM109	The Vendor staff should adhere to all Department security requirements when on-site at Department facilities and as required by the facility's security requirements.	Security Management
FDGS agrees that all staff will adhere to all Department security requirements when on site at Department facilities and as required by the facility's security requirements.		
SM110	The Vendor should protect the Vendor's data center location(s) against intrusion at all times and maintain a surveillance alarm system that is linked to a manned monitoring center.	Security Management
Fiserv maintains highest level of data center security to protect our locations against intrusion at all times. We maintain a manned monitoring center with surveillance alarm systems. Physical access to our systems and facilities are restricted to authorized individuals only. Access to the Cyber Vulnerability Center is maintained, administered, and controlled by Corporate Security. Additionally, an electronic record is maintained by Corporate Security of access to secured areas.		
SM111	The Vendor should provide the Department access to all facilities to conduct announced and unannounced visits of the Vendor's facilities.	Security Management

Req. ID #	Requirement Text	Requirement Type
To maintain security controls at our facilities, visits must be scheduled and approved prior to arrival. This is to maintain the auditable access controls of our facilities for the security and protection of all Fiserv clients supported in our data centers. As part of Fiserv, AuthentiCare is subject to multiple governmental security reviews including federal banking (FFIEC), credit card (PCI), and federal privacy (GLBA). While not directly applicable, as AuthentiCare does not process credit cards or financial transactions for example, these standards speak to the level of security and privacy expected for all Fiserv applications and our facilities and infrastructure.		
SM112	The Vendor should maintain a current database of individuals who have access to its facilities and the database should be available for the Department's inspection upon request.	Security Management
Our policy does not allow facility access details to be distributed outside of Fiserv. As noted in SM110, physical access to our systems and facilities is restricted to authorized individuals only. Access to our data centers is maintained, administered, and controlled by Corporate Security. Electronic records are maintained by Corporate Security of access to secured areas.		
SM113	The solution should have the ability to reassign existing records from one user identifier (ID) to another user ID in the case of fraud, errors, and omissions that affect data integrity and reporting according to the Department's business rules. All reassignment of records should be captured in audit logs.	Security Management
As an exception to normal data management, our FDGS technical support team will execute a series of scripts to reassign existing records from one user identifier (ID) to another user ID in the case of fraud, errors, and omissions that may affect data integrity and reporting. The use of scripts is necessary to cause database updates to be captured in the standard AuthentiCare audit logs.		
SM114	The solution should audit and track all activity specific to each user including, but not limited to:	Security Management
SM115	Invalid login attempts	Security Management
SM116	Transaction activities	Security Management
SM117	Track adds, changes, and deletes of individual member visit verification data	Security Management
SM118	Password changes	Security Management
SM119	Security question and/or Key creation	Security Management
SM120	Updates to security questions	Security Management
SM121	User navigation history	Security Management
AuthentiCare maintains a full audit trail of all data modifications to the data item level including what was changed and how it was changed, and displays a summary of who made edits and when. AuthentiCare audit reporting includes, for example, a Claim History report to show more details of edits and changes and to support viewing of claim notes added to each record. Online history reports are available for EVV visits and authorizations, while audit records for other data (Services, Clients, Providers, Caregivers, Schedules, and others) are maintained and available from FDGS. FDGS maintains operational logs of system activity of each web service transaction to AuthentiCare from the Mobile App for the past 30 days. Additional operational audit trail details support the tracking of login attempts, password changes, and related security question updates. These are also used to investigate any issues the users may have had with operating the system. Audit logs cannot be modified.		
SM122	The Vendor should ensure that its employees and subcontractors complete and maintain required security training and follow State and Department policies regarding security. This should be done, at a minimum, on an annual basis and for all new hires within five (5) business days of being hired (Reference: https://www.wv.gov/Policies/Pages/default.aspx#undefined)	Security Management

Req. ID #	Requirement Text	Requirement Type
FDGS has examined the policy noted in this requirement and agrees to complete and maintain the appropriate training for our employees and contractors. Each staff member receives instruction on Personal Identifying Information (PII) and Protected Health Information (PHI) security and privacy policies and procedures and, upon hiring, is required to sign an agreement with the company to uphold them. All employees and contractors are required to comply with security and privacy training requirements on an annual basis. Any transgression against our procedures is met with immediate response from management and disciplinary action according to corporate policy.		
SM123	The solution should collect sufficient detail to produce an immutable audit log of all manual and automated system activity including, but not limited to the following elements:	Security Management
SM124	User Identification	Security Management
SM125	Machine/Internet Protocol Address Identification	Security Management
SM126	Time and Date of Action	Security Management
SM127	Actions Performed	Security Management
The AuthentiCare EVV platform maintains an immutable audit trail of data record creation and updates. Online history reports are available for EVV visits and authorizations, while audit records for other data (Services, Clients, Providers, Caregivers, Schedules, and others) are maintained and available from FDGS. FDGS maintains operational logs of system activity of each web service transaction to AuthentiCare from the Mobile App for the past 30 days. These are also used to investigate any issues the users may have had with operating the system. Audit logs cannot be modified. Manipulation by database administrators are strictly monitored and are only permitted through formally approved data change requests.		
SM128	The solution should record an immutable audit log of security role assignment and revocation activities performed within the solution and changes to security role assignments on servers and in databases	Security Management
User role assignments, changes, and revocations within the EVV solution are part of the AuthentiCare audit trail. Fiserv has established a series of products and methods for "hardening" the hardware and software infrastructure including access to all servers and databases. Users accessing non-public information on Fiserv systems, whether from internal or external network locations, are identified and authenticated to the authorized environment. Access and changes to security role assignments of all servers, databases, and related system components are monitored and tracked for audit purposes.		
SM129	The Vendor should disable building and system access in real-time for staff upon termination, departure, or reassignment from the project.	Security Management
Termination, departure, and reassignment requests are processed automatically by our identity management system, using a daily feed from the HR system into the identity management system. The identity management system updates each terminated user's Active Directory profile description field with the termination date as a reference. After 90 days, the disabled accounts are permanently deleted from Active Directory.		
SM130	The solution should generate audit reports based on a request from authorized requestors at the Department.	Security Management
The AuthentiCare EVV platform maintains a full audit trail of data record creation and updates. Online history reports are available for EVV visits and authorizations, while audit records for other data (Services, Clients, Providers, Caregivers, Schedules, and others) are maintained and available from FDGS. FDGS will work with the Department for other audit report requests from authorized representatives of the Department. Depending on the report details requested, additional technical resources may be required.		
SM131	The solution should have the ability to control access to member records based on user roles and system credentials.	Security Management
Each AuthentiCare user of the web portal and mobile app is granted specific role-based access through the use of a unique user ID. AuthentiCare's role-based security supports a hierarchical structure in which users are granted access to specific areas, functions, and data within the product. Users are assigned to roles which are assigned specific rights to access within the system.		
SM132	The solution should support member-delegated authority including, but not limited to:	Security Management

Req. ID #	Requirement Text	Requirement Type
SM133	Assistors	Security Management
SM134	Authorized representatives	Security Management
AuthentiCare supports the definition of additional user roles that will allow member-delegated authority including Assistors and Authorized Representatives. Authorized Representative user roles and functionality is established in other state implementations of AuthentiCare for EVV. FDGS will begin with existing role definitions to verify the user-based access requirements of these roles during the iterative design and configuration sessions.		
SM135	The Vendor should require that all employees accessing sensitive and critical member data successfully pass State and Federal fingerprint-based background checks prior to potential or actual data access. See request for proposal (RFP) Section 3: General Terms and Conditions for more information.	Security Management
FDGS recognizes the importance of and reliance on secure and proper staff authorizations in the context of any large project. In accordance with contract requirements, FDGS will comply with all State and FDGS contractual and legal requirements, including signed confidentiality policies/agreements and fingerprint-based, criminal background checks. All new hires at Fiserv must pass a background check prior to employment. The background check is the last step after a candidate has passed through all interviews prior to starting with the company. Fiserv will perform background checks on its employees and on certain non-employees (a) with unescorted physical access to the company's premises or (b) who are issued a user name and password to access information technology systems on which Client Data are stored or accessed, or who have any other logical access including 1DC or LAN access. For employees hired after November 1, 2006, the background checks will, to the extent not prohibited by applicable law, extend back 10 years from the date of the background check. Fiserv will not knowingly allow any employee or subcontractor's employee who has been convicted of a felony Crime of Dishonesty during the period of the background check or thereafter to perform services for Fiserv. We will also perform or cause to be performed screening for illegal drug use on Fiserv employees and certain non-employees.		
SM136	The Vendor should conduct information security assessments and audits of the solution to be conducted by the Vendor, by the Department, or by an external entity hired by the Department as directed by the Department.	Security Management
Fiserv's Unified Vulnerability Management Services (UVMS) Team's primary responsibility is to perform periodic penetration tests and vulnerability assessments of Fiserv's infrastructure and applications. UVMS plays a vital role in helping to protect customer information and the assets of FDGS. UVMS employs a variety of technologies, tools, and techniques to help confirm that high-quality security assessments are performed. Security assessments identify vulnerabilities that may represent varying degrees of risks to Fiserv. Vulnerabilities deemed of risk to Fiserv are assigned to appropriate individuals who are required to take action to mitigate any risks associated with identified vulnerabilities. **Assessments** *Penetration Testing:* Penetration testing is conducted to comply with Fiserv policy, customer mandates, and Payment Card Industry Data Security Standard (PCI-DSS) requirements. The purpose of penetration testing is to measure the security posture of a target system or environment. Penetration testing is not simple hacking but, instead, is a process designed to validate security weaknesses, identify attack vectors, and validate the functionality of security controls. The penetration testing process used by Fiserv is a 'gray' box approach as defined in NIST 800-115 *Technical Guide to Information Security Testing and Assessment*. Penetration tests are designed to be non-destructive, and minimize the potential impact to systems or networks under test. *Third-Party Penetration Testing:* UVMS facilitates an annual third-party security assessment of external networks. These tests are performed in addition to UVMS testing, and are executed by an approved, independent third party. Only GCSF-approved vendors are authorized to execute testing on Fiserv's behalf, in accordance with Fiserv policy. *Vulnerability Scans:* A vulnerability scan is an automated process that is designed to assess computers, computer systems, networks, or applications for security vulnerabilities or weaknesses. While functionality varies between different types of vulnerability scanners, they share a common, core purpose of enumerating the vulnerabilities present in one or more targets. In accordance with Fiserv policy, UVMS uses Nessus and Trustkeeper to perform regular vulnerability scans of Fiserv's network and computer systems. The scanning tools used are considered industry standard and are customized to test Fiserv networks in an efficient manner, while minimizing the potential risks associated with active scanning.		

Req. ID #	Requirement Text	Requirement Type
Vulnerabilities deemed of risk to Fiserv are assigned to appropriate individuals who are required to take action to mitigate any risks associated with identified vulnerabilities. Fiserv UVMS tracks and reports on results of the security assessments performed. Results of ad hoc assessments performed outside of normal testing cycles are provided to the requester, system owner, and the Cyber Risk Manager responsible for the network or system under test. Physical access to UVMS systems and facilities is restricted to authorized individuals only. Access to the Cyber Vulnerability Center is maintained, administered, and controlled by Corporate Security. Additionally, an electronic record is maintained by Corporate Security of access to secured areas.		
SM137	The Vendor should conduct all security, privacy, and/or risk assessments inclusive of vulnerability scans of the solution and the results of the vulnerability scan should be included with the assessment results.	Security Management
In accordance with Fiserv policy, security, privacy, and risk assessments are conducted at least annually. Fiserv provides security reporting through our audited SOC 1/SOC 2 assessment reports *Third-Party Penetration Testing:* UVMS facilitates an annual third-party security assessment of external networks. These tests are performed in addition to UVMS testing, and are executed by an approved, independent third party. Only GCSF-approved vendors are authorized to execute testing on Fiserv's behalf, in accordance with Fiserv policy. *Vulnerability Scans:* A vulnerability scan is an automated process that is designed to assess computers, computer systems, networks, or applications for security vulnerabilities or weaknesses. While functionality varies between different types of vulnerability scanners, they share a common, core purpose of enumerating the vulnerabilities present in one or more targets. In accordance with Fiserv policy, UVMS uses Nessus and Trustkeeper to perform regular vulnerability scans of Fiserv's network and computer systems. The scanning tools used are considered industry standard and are customized to test Fiserv networks in an efficient manner, while minimizing the potential risks associated with active scanning. Vulnerabilities deemed of risk to Fiserv are assigned to appropriate individuals who are required to take action to mitigate any risks associated with identified vulnerabilities. Fiserv UVMS tracks and reports on results of the security, privacy, and risk assessments performed, inclusive of vulnerability scans. Results of scheduled and ad hoc assessments performed outside of normal testing cycles are provided to the requester, system owner, and the Cyber Risk Manager responsible for the network or system under test.		
SM138	The Vendor should allow for only Department approved users to enter and/or approve change request activities, per the Change Management Plan.	Security Management
FDGS agrees to only allow authorized Department personnel to enter and/or approve change requests and related change request activities. FDGS will document the Change Management Plan as a sub-plan to the complete Project Management Plan (PMP). After a walkthrough of the Change Management Plan, it will be submitted to the Department as Deliverable D002 for review and approval. Authorized Department personnel may be included in the Change Management Plan.		
SM139	The solution should comply with the standards and protocols under sections 1104 and 1561 of the Affordable Care Act (ACA). (Reference: https://www.caqh.org/core/operating-rules-mandate) (Reference: https://www.healthit.gov/sites/default/files/rules-regulation/aca-1561-recommendations-final2.pdf)	Security Management
Along with the requirements of the 21st Century Cures Act, AuthentiCare complies with ACA Sections 1561 and 1104 regarding HIPAA security and privacy standards. FDGS gives highest priority to protecting the security and privacy of Department data, and the environment that houses it. FDGS has a critical role in maintaining the Department's overall compliance with security and privacy laws, regulations, and CMS standards. AuthentiCare complies with HIPAA (and HITECH) practices and requirements. The AuthentiCare platform provides world-class security with a proven track record for proactive security and privacy protection.		
SM140	The Vendor should follow Federal, State, and Department policies for receipt and removal of hardware and electronic media that contain electronic protected health information according to 45 CFR164.310. (Reference: https://www.hhs.gov/sites/default/files/patient-protection.pdf)	Security Management
Fiserv/FDGS follow Federal, State, and Department policies for receipt and removal of hardware and electronic media that contain electronic protected health information according to 45 CFR164.310.		

Req. ID #	Requirement Text	Requirement Type
SM141	The solution should allow local and central system security administrators to add and change permissions for local and central system access.	Security Management

Role-based access to the AuthentiCare web and mobile application is managed by state and provider administrators.

Access to certain sensitive areas (for example, data centers, computer rooms, network command centers) where AuthentiCare is hosted, is managed centrally and must be authorized by the management of those facilities. New employee and contractor access and changes to existing access for facilities is granted based on authorized requests. Global Identity & Access Management (GIAM) personnel are directly responsible for granting access within enterprise authentication and authorization systems. Significant examples include the mainframe, VPN, and web access management systems, by creating access rules in the CA-Top Secret, distributed systems, and VPN access databases.

SM142	The Vendor should maintain the same level of security compliance during any interruption of normal operations as outlined in the RFP Contract Deliverables and applicable federal requirements.	Security Management

FDGS agrees to maintain the same level of security compliance during any interruption of normal operations. The Fiserv security plan is fully developed and in operation today, driven by highly experienced security staff who maintain up-to-date standards and policies with respect to market changes and system requirements. The plan encompasses the full AuthentiCare platform environment including both our primary and secondary (backup) facilities. FDGS will verify that all EVV data necessary to perform the duties as outlined in this RFP are stored in a secure and confidential manner that meets federal and state rules and regulations, including HIPAA/HITECH compliance.

FDGS' system security applies our "Defense in Depth" approach incorporating an extensive combination of physical, technical, and administrative controls. This multi-layered approach to securing AuthentiCare EVV data is reviewed and approved by multiple independent assessors. Critical areas addressed include:

- System access security
- Network security
- Application design and security
- Physical access security
- Data security and encryption

SM143	The solution should have the ability to securely access all data in the event of an emergency without any impacts to the confidentiality or integrity of the data.	Security Management

To securely access all data in the event of an emergency, the EVV solution will use the AuthentiCare platform within Fiserv's secure, redundant, and highly available hosted environment. Fiserv hosts a "captive cloud" solution that provides the scalability benefits of a cloud solution. So that our solution is always available, Fiserv operates parallel data centers in geographically diverse locations, with the primary site located at Chandler, Arizona and the secondary site located in Omaha, Nebraska. Fiserv maintains fully documented policies and procedures for Disaster Recovery and Business Continuity.

In the event of a disruption of service to the primary site, the secondary site assumes processing of the additional workload, allowing users to continue execution of service without outages or delays. Figure 7.13 depicts the data center redundancy supporting our Disaster Recovery and Business Continuity Plans.

Req. ID #	Requirement Text	Requirement Type

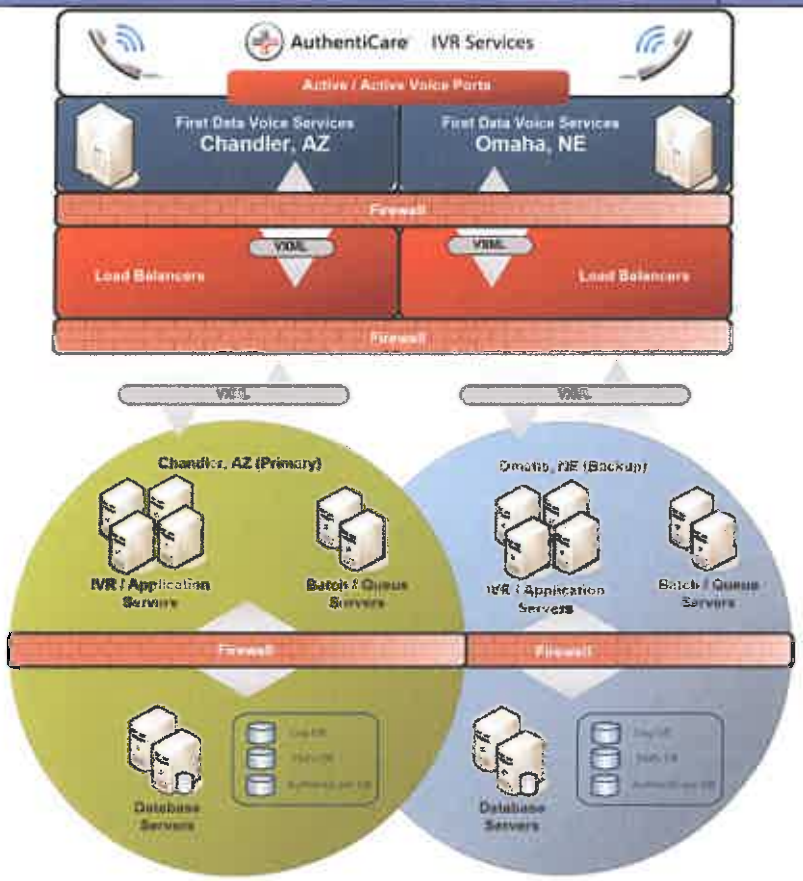


Figure 7.13 – Data Center Redundancy Maintains Access During an Emergency

With data center redundancy and real-time transaction replication of data between data centers, most operating contingencies that arise can be mitigated by re-routing data traffic until the issue is resolved.

Data backups collected from the AuthentiCare system are securely stored at geographically dispersed networked data backup locations spread across Fiserv facilities as an extra safety measure. The backups are encrypted and networked across a distributed storage infrastructure so that the data never leaves a secure Fiserv facility and captive network, but maintains redundancy across facilities so data are protected from loss at any one facility. This eliminates the need for offsite storage using magnetic media that requires secure handling and storage and has to be sanitized according to NIST SP 800-88.

The AuthentiCare platform is built on a distributed architecture where many servers perform individual functions within the solution. Each server may have its own distinct recovery process based on the function it performs.

By hosting the solution with Fiserv, the Department will have the confidence that every check-in and check-out will be accurately recorded and stored in a highly secure environment that meets the requirements of the state in the event of a disaster.

SM144	The Vendor should deliver the system architectural activity and process diagrams that detail security and privacy controls to the Department upon request.	Security Management
We will meet this requirement with the appropriate proprietary controls in place. The requested system architectural activity and process diagrams that detail security and privacy controls are considered proprietary and confidential. If awarded, FDGS asks to review this and similar requirements asking for proprietary AuthentiCare system details that cannot become public domain.		
SM145	The Vendor should ensure that all Vendor-owned hardware and software are configured securely, including but not limited to:	Security Management

Req. ID #	Requirement Text	Requirement Type
SM146	Being protected by industry standard virus protection software, which is automatically updated according to a Department-approved schedule.	Security Management
SM147	Having all security patches installed that are relevant to the applicable operating system and all other system software and hardware.	Security Management
SM148	Maintaining compatibility with Department software and systems.	Security Management
SM149	Utilizing only licensed software and hardware solutions that have not been classified as End-of-Life (EOL).	Security Management

FDGS confirms that all hardware and software needed for the AuthentiCare EVV solution is securely configured.

Virus Protection
Antivirus and Malware software is controlled by Endpoint Security, which is installed by default on Windows and UNIX/Linux servers, laptops, and workstations. Updates are pushed from the central management system automatically as they are released. Malware events of interest are escalated to the cyber security incident response team and are handled in accordance with established processes and procedures. Antivirus and malware software is administered by IT Support on every Windows and UNIX/Linux server, workstation, and laptop upon issuance, and only IT Administrators have access to disable the software.

Security Patches
Fiserv receives up-to-the-minute information pertaining to the cyber threat landscape (including vulnerability announcements, data on patch and non-patch remediation, and emerging threats that correspond to applications and system inventory).

From a network perspective, secure, encrypted communications are used for remote administration of production systems and applications. System standards/procedures include disabling all unneeded or unused services. There is a formal process and schedule for testing and implementing security-related patches.

Software and System Compatibility
Our data center staff, architects, and product team examine compatibility with all potential hardware and software upgrades.

Licensing and End-of-Life Status
Fiserv maintains all hardware and software licenses necessary to host and run the AuthentiCare platform. Our data center staff identify license expiration dates to make sure that all hardware and software remains within active support timeframes.

SM150	The Vendor should ensure they are in compliance with the State and Department Information Technology Security and Privacy Policies.	Security Management

FDGS provides EVV services in a multi-client environment. As a result, FDGS cannot follow or adapt to the differing and perhaps conflicting requirements of its customers. FDGS must maintain its current practices and process in place to maintain a consistent and coherent approach based on FDGS' knowledge and experience of its processing environment. FDGS has examined publically available State and Department Information Technology Security and Privacy Policies. We feel that our solution meets or exceeds compliance requirements.

We maintain a documented security plan that is regularly audited by the FFIEC, our Payment Card Industry (PCI) assessor, and under SSAE-18 by Ernst and Young. FDGS security plans and procedures are prepared at a facility level, and the solution is hosted in large-scale, redundant data centers with Department data housed separately from other customers' data. Use of the SSAE-18 exceeds the requirement for the SSAE-16 Type 2 audit.

Corporate security policies also include practices in FTC 16 CFR Part 314, Standards for Safeguarding Customer Information; Final Rule. Certified controls from PCI-DSS and SSAE-18 map to and cover applicable HIPAA security controls as specified in NIST SP800-66 r1 Appendix D: *HIPAA Security Rule Standards and Implementation Specifications Crosswalk*.

FDGS will continue to maintain third-party SSAE-18 and PCI certification during the term of the contract. FDGS will provide the Department with a copy of the PCI compliance certificate and executive summary of the SSAE-18 report. Report details are considered confidential and cannot be subject to FOIA discovery and disclosure. The Department may request copies of the SOC 1/SSAE-18 reports.

SM151	The Vendor should maintain documentation of encryption keys, interface credentials, and service account credentials, and provide the Department with updated documentation every time an update is made.	Security Management

Req. ID #	Requirement Text	Requirement Type
The requested documentation of encryption keys, interface credentials, and service account credentials are considered proprietary and confidential. If awarded, FDGS asks to review this and similar requirements asking for proprietary AuthentiCare system details that cannot become public domain. We will meet this requirement with the appropriate proprietary controls in place.		
SM152	The Vendor should provide continuous monitoring of the solution using intrusion detection software (IDS).	Security Management
Fiserv provides continuous monitoring using intrusion detection software (IDS). Intrusion Detection is in place on the following segments: Internet point-of-presence, DMZ, Extranet, internal production network, and network segment hosting target data. It is configured to generate alerts in case of incidents and values exceeding normal thresholds for the environment. A formal process is in place to regularly update the Intrusion Detection System (IDS) signatures based on new threats and changes in the environment. The system is monitored 24x7x365. IDS events feed into the Incident Management process that alerts operations personnel to take action to resolve the issue.		
SM153	The Vendor should provide reports at intervals as agreed upon by the Bureau from the intrusion detection software (IDS).	Security Management
Network Intrusion Detection Software (NIDS) events feed into the Incident Management process that alerts operations personnel to take action to resolve the issue. FDGS agrees to follow the mutually agreed-upon Incident Management reporting requirements.		
SM154	The Vendor should provide continuous monitoring of the solution using industry standard intrusion prevention software (IPS).	Security Management
Internet connectivity to the Fiserv network is continuously monitored by data center staff. The Fiserv network is protected by a firewall complex that uses leading commercial firewalls and various IDPS and techniques (IDPS.01). There is one type of firewall in use across Fiserv in North America. Firewalls are managed by approved firewall administrators. Each firewall cluster consists of two redundant firewall devices, to provide hot failover protection. All firewall devices are hosted in the Fiserv Omaha and Chandler data centers.		
SM155	The Vendor should provide reports at intervals agreed upon by the Department from the intrusion prevention software (IPS).	Security Management
Network Intrusion Detection Software (NIDS) events feed into the Incident Management process that alerts operations personnel to take action to resolve the issue. FDGS agrees to follow the mutually agreed Incident Management reporting requirements.		
SM156	The solution should have the ability to support non-disclosure of information.	Security Management
AuthentiCare offers both user authentication as well as role-based user profiles to make sure that only information that is required by each role is accessible. In addition to authenticated and authorized access to EVV information, all data are encrypted so that it is not accessible outside of the AuthentiCare application. The mobile application also disables the screen shot capabilities of the device to prevent images of EVV data. For example, AuthentiCare is designed to automatically mask sensitive data displaying only the last four digits on screens and reports.		
SM157	The Vendor's Technical Call Center should have the ability to authenticate the caller/user as required by the Department.	Security Management
FDGS will work with the Department to compile an authorized user list including email address, phone number, and other required data necessary to authenticate callers to the Technical Call Center.		
SM158	The solution should provide complete logical and physical segregation of electronic visit verification (EVV) data and files from the data and files of other Vendor/Vendor customers.	Security Management
Data for each AuthentiCare statewide implementation is stored in a database dedicated to that client. West Virginia will have its own database so there is no comingling of EVV data. Each AuthentiCare client is assigned a unique URL for access to the web portal and unique toll-free number for IVR-based visit capture. Web service interactions require specific customer authentication. Batch files require proper customer naming conventions for receipt and processing.		

8.0 Attachment 9: Implementation Specifications Approach

RFP Section 5.4.2.10 (Table 11), Attachment 9, 4.4.3, pp. 74, 121, 53
1.1 The Vendor should provide a narrative overview of how the proposed system will meet the specifications and narrative in this request for proposal (RFP).
1.2 Use these response sections to provide specific details of the proposed approach to meeting the implementation specifications in each process area. Be advised, while some sections only require narrative around specifications others may also contain pointed questions.
1.3 Responses should reference specifications and relevant mandatory requirements using the appropriate IDs from Appendix 1: Detailed Specifications and Attachment 6: Mandatory Requirements.
1.4 Responses in the sections below should be focused on the Department of Health and Human Resources (DHHR) business processes and requirements. DHHR also expects the Vendor to propose its approach for meeting the narrative included in this RFP.
1.5 The Vendor is required to respond to the headings below to provide detail regarding its methodology for each project management component.

FDGS provides DHHR with its AuthentiCare implementation methodology that has proven successful across seven other statewide EVV deployments for projects of similar size and scope.

FDGS recognizes that West Virginia is seeking an Electronic Visit Verification (EVV) system that already meets the requirements of the 21st Century Cures Act, as well as the objective to satisfy CMS certification requirements to maximize federal matching funds. We also understand the importance of meeting the upcoming deadline for 21st Century Cures Act Good Faith Extension (GFE) compliance by January 2021 to avoid FMAP penalties.

We propose an expedited implementation "Phase 1" that focuses on those requirements necessary to comply with the Cures Act and fully support the CMS certification criteria. Along with the detailed implementation specifications included in this section for Project Management and Training, we provide the Department with descriptions of our approach to the implementation and deployment for the AuthentiCare EVV solution in West Virginia.

At all times, we understand that EVV systems require CMS certification. We continue to support our other EVV customers and work with them and CMS to prepare for the latest Outcomes Based Certification process. We have updated our project work plan and related methodology to remain current with CMS guidance. For example, AuthentiCare EVV solution meets the requirements of 21st Century Cures Act with the necessary data collected to be compliant, but also captures the data elements needed to report on the Outcomes Based Key Performance Indicators ongoing.

Once "Phase 1" has been deployed and West Virginia's EVV system is compliant with the Cures Act, FDGS will already be working on the scope planned for the next phase and release. This approach continues our iterative design, configuration, and testing cycles that we call Contract Milestones. Depending on the size of each release, one or more Contract Milestone cycles will be included with demonstrations of the enhanced EVV system presented to the Department near the completion of each milestone.

Our flexible solution is built to gather all of the visit verification data necessary for EVV programs today. The configurable solution allows us to quickly prepare AuthentiCare to support DHHR's EVV program policies and procedures. No matter how caregivers check in and out of

AuthentiCare, our solution verifies each of the data elements required by the 21st Century Cures Act for each service.

The AuthentiCare EVV solution is currently operational in seven statewide and other consumer direct implementations, similar in size and scope to West Virginia's requirements. Our approach focuses on the capabilities already available within AuthentiCare to achieve the goal of complying with 21st Century Cures Act and the latest Outcomes Based Certification (OBC) from CMS.

The subsections below address the complete EVV solution provided by FDGS from Kickoff to CMS Certification for West Virginia.

8.1 Project Management Methodology

RFP Section Attachment 9 – 2-2.8.3, 4.4.3.1, pp. 121, 53
2.1 The Vendor's proposal should describe the Vendor's methodology, tools, and techniques used to support projects from requirements through finished deliverables, including deployment of the new solution, project management, checkpoints, and periodic status reporting.
2.1.1 Describe policies and procedures employed to ensure timely completion of tasks in a quality fashion.

Project Management Methodology, Tools, and Techniques

As described in Proposal Section 4.0 Attachment 5: Initial Work Plan, FDGS offers a proven approach to validate the EVV requirements, iteratively complete the desired system configuration based on the approved design, and take our customers through AuthentiCare user training in preparation for Go Live and ongoing Maintenance and Operations.

As noted with our Initial Work Plan and other sections, our team will follow our implementation methodology to meet an aggressive six-month implementation schedule to comply with the 21st Century Cures Act deadlines and the implement the functionality to complete CMS certification. Prior to the end of the initial implementation period, FDGS will work with the Department to complete the plans for the next and future releases of AuthentiCare, adding more and more of the required features and functions agreed to in this RFP.

2.3 Work Plan
2.3.1 The Vendor's proposal should supply a narrative describing the Vendor's proposed processes and methodologies for providing the scope of work described in this RFP. Include any assumptions as well as the Vendor's approach to meeting the Initial Work Plan. The Vendor should include detail sufficient to give DHHR an understanding of how the Vendor's knowledge and approach will:
2.3.1.1 Manage the work
2.3.1.2 Guide work execution
2.3.1.3 Document planning assumptions and decisions
2.3.1.4 Facilitate communication among stakeholders
2.3.1.5 Define key management review as to content, scope, and schedule
2.3.2 The Vendor should also submit an Initial Work Plan in Attachment 5: Initial Work Plan that demonstrates that the Vendor has a thorough understanding of the scope of work and project requirements.

Project Work Plan

Proposal Section 4.1 includes our initial project work plan and work breakdown structure. We begin with a plan and schedule that has proven successful in our other statewide EVV projects and then tailor it specifically to the scope and timeline of this RFP. Early project activities validate the existing project components and then add to the specific updates needed once the project requirements are validated and approved.

The project schedule is a living document managed by the FDGS Project Manager. The approved Change Management Plan describes those items that allow for changes to the work plan. The Project Manager provides regular status updates to DHHR leadership as required. Additional metrics are tracked and reported to clearly communicate project progress according to plan and related issues and risks that could impact the schedule.

2.4 Issue Management
2.4.1 The Vendor's proposal should describe the Vendor's process for issue management, including: issue logging, resolution, tracking of unresolved problems, escalation procedures, closeout, and reporting practices.
2.4.2 The Vendor should describe its proposed approach for integration of issue management across sub-contractors, if applicable, as well as other DHHR and Vendor project stakeholders.
2.4.3 The Vendor should also detail any planned use of an automated solution to support issue management.
2.5 Risk Management
2.5.1 The Vendor's proposal should describe the Vendor's risk management practices, the expected risk areas,

and mitigation plans.
2.5.2 In addition, the response should elaborate on the Vendor's internal risk management plan. This should include reference to the use of any specific methodologies, as well as any specific tools being used.

Risk and Issue Management

Please see Proposal Section 4.2.11 Risk Management Plan. FDGS has included an abridged description of our Risk Management Plan (RMP) as part of the Project Management Plan (PMP). The RMP follows PMBOK guidance from initial risk identification through the risk process workflow to analysis, responses, monitoring and controlling, and effectively communicating to the Department through the weekly status meetings and monthly status reports. With our experience, FDGS is able to share risks and lessons learned from similar EVV projects along with how we previously mitigated or eliminated each risk. This provides the Department with a project team that knows what is ahead in the schedule with our proven approach to the implementation phases and activities.

Similar to the Risk Management Plan, the draft Issue Management Plan assumes coordination and reporting through the FDGS Project Manager and team members. During project initiation, we will work with the Department to provide the updated Issue Management Plan, designating and assigning FDGS roles and responsibilities specific to the EVV project and issue management.

The issue management process consists of the steps listed below, which are described in the Issue Management Plan subsections, Issue Identification and Documentation:

- Identification/Documentation
- Validation, Assignment, and Prioritization
- Analysis
- Tracking and Reporting
- Issue Escalation Process
- Resolution and Closure

2.6 Quality Management
2.6.1 The Vendor's proposal should describe the Vendor's approach to ensure the quality of the solution and include details on the management of requirements through traceability matrices, Configuration management activities, organizational readiness, and deliverables and artifacts.
2.6.2 The Vendor's approach should also detail information on the proposed quality metrics as well as the Vendor's approach to managing solution defect and issue tracking.
2.6.3 More specifically, the Vendor's approach to quality management should include, at a minimum, the following elements:
2.6.3.1 Management of the solution specifications. This includes the identification of inconsistencies between the specifications, project deliverables, and/or artifacts.
2.6.3.2 Management of the Requirements Traceability Matrix (RTM) that will be used for specifications management. This includes detail on how the quality management approach will support maintain the traceability between the specification and the proposed solution.
2.6.3.3 Management of configuration management activities, including but not limited to the control and monitoring of the software library.
2.6.3.4 Management of practices and procedures that will be followed for reporting, tracking, and resolving problems or issues identified in the solution's development, transition, and maintenance.
2.6.3.5 The Vendor's approach to business process changes resulting of requests from DHHR.
2.6.3.6 The Vendor's approach to an organizational readiness assessment of DHHR's organization. This may include a gap analysis and recommendations for organization change required to support the solution's implementation in DHHR environment. This assessment should be approved a minimum of three (3) months prior

to the solution's deployment.
2.6.3.7 The Vendor's approach to the quality of work products developed and delivered by Vendor and the Vendor's subcontractors, if applicable.
2.6.3.8 The Vendor's proposed quality management approach should include detail on how the Vendor plans to deliver signature ready project deliverables. The Vendor should assume DHHR will complete its review of signature ready deliverables within ten (10) business days.
2.6.3.9 The Vendor's approach to how quality metrics and measurements will be identified, collected, and analyzed to ensure that quality goals, including management and DHHR solution goals, are being met. It should also describe the types of project metrics used.
2.6.3.10 The Vendor's organizational structure, and the roles and responsibilities of Vendor staff as they relate to quality management.
2.6.4 The Vendor's description of the processes and approach to manage solution defect and issue tracking solution for tracking and resolution of items and, if applicable, how the quality management approach will support corrective action plans (CAPs) being developed to address more significant issues.

Quality Management

FDGS follows a disciplined Quality Assurance (QA) approach that contributes to our record of delivering projects on time, within budget, and with high quality. This is a process of quality review for each project milestone deliverable. FDGS conducts internal peer-to-peer quality reviews to provide "complete" deliverables prior to submission for approval. This submission to DHHR will include joint review of the deliverable as needed and signoff "passed" as agreed to in the project management plan.

FDGS creates the Requirements Traceability Matrix (RTM) to preserve line of site from specification to end solution. It does this based on the requirements of the RFP. The RTM is the tool that we use to establish the format, scope, and system for tracking requirements. RTM system and software specifications must be correct, complete, traceable, and testable.

Once the RTM is complete, additional details will be identified during application Design Sessions at the beginning of the project. The RTM is then jointly reviewed and updated during the project meetings throughout the initiation and planning phases. As the project moves into the different testing phases, the requirements are traced through the RTM for ongoing tracking and reporting of project progress maintaining line of site to the original specification.

As part of the quality management oversight, modifications resulting from business process changes during the life of the project or those derived from gap analysis in design will be managed following the Change Management Plan guidelines. Issues that arise needing corrective action are resolved using project management best practices as described in the Project Management Plan agreed to at the start of the project.

As the project moves towards completion, FDGS will coordinate pre-production release management activities and establish resource planning and tracking processes. As part of that the FDGS Project Manager is the owner of all schedule updates and reporting. We include schedule updates and tracking metrics in our regular weekly status meetings and monthly project status reports. This frequency allows for consistent and frequent updates as well as clear identification of any schedule risks or issues that could impact schedule progress.

Our approach to the EVV project is documented in the plans and processes of the Project Management Plan (PMP), each sub-plan lays out the approach to the key steps and methods we use to execute each phase of the project from Kickoff, design and configuration and development, testing, training, and preparation for Go-Live, to the final transition to ongoing Operations and Maintenance. Early on in the planning process, FDGS will work with DHHR to determine the organizational needs for deployment and transition to production. This includes a

gap analysis and assessment to identify training and communication needs to be implemented to support the transition to production.

Quality metrics are collected throughout the project lifecycle by archiving artifacts in the various lifecycle tools in use. This includes the Confluence and Jira portals, as well as our CLM Defect management system.

Throughout the duration of the EVV Project, FDGS reviews design deliverables, code, and quality assurance test cases. The internal quality assurance measures include:

- **Self-Review:** Any individual responsible for a work product, deliverable, or deliverable component will use a quality assurance checklist to evaluate the item's readiness. This checklist contains the standards for that specific deliverable as delineated in the contract or as otherwise identified. The individual will measure the deliverable against the checklist standards and repeat the review as necessary until conditions are met.
- **Peer Review:** As a secondary quality assurance review, specific design documents and deliverables will undergo a cross-functional peer review that focuses on the overall item completeness, with an emphasis on observations and recommendations.
- **Project Team Lead Review:** An AuthentiCare product team lead will review project deliverable documents for acceptability.
- **Technical Lead Code Review:** The Technical Lead assigned to the project will review any custom code that the programmers add to the AuthentiCare solution.
- **Additional Review Cycles:** As an additional quality assurance review, the Product Manager, Project Director, Executive Oversight, or SMEs will review specific work products and deliverables with a focus on comprehensive content and overall completeness of the item.

A component of the Quality Management discipline is the Testing Center of Excellence. FDGS has a dedicated team of testing subject matter experts that comprise our Testing Center of Excellence (TCoE) pool of resources. The TCoE is equipped with the processes, technology, tools, infrastructure, and talent to support quality deliverables. The project team will work closely with TCoE resources to provide the highest level of quality assurance throughout the entire lifecycle of the project.

FDGS will identify and remediate defects in all phases of the project. Quality for AuthentiCare delivery is verified through the following:

1. Conducting design review sessions to identify any potential risks to the current production system
2. Conducting code reviews
3. Verifying that the Business Requirements provided were thoroughly tested
4. Regression testing the application to identify unexpected defects caused as a result of the new requirements
5. Engaging with and supporting the client to participate in Customer User Acceptance testing
6. Completing Software Testing Activities within project schedule parameters

To successfully meet the goals and objectives of quality management, our approach for effective project control is based on the application of proven industry standards, techniques, and methodologies derived from:

- **International Standards Organizations (ISO):** For FDGS, meeting customer needs goes beyond creating and delivering innovative quality products. We have staff who understand the technical, practical, and operational details relevant to each implementation supporting our solutions. FDGS emphasizes ISO's seven quality management principles:
  - Customer focus
  - Leadership
  - Engagement of people
  - Process approach
  - Improvement
  - Evidence-based decision making
  - Relationship management

  These form a basis for quality performance improvement and organizational excellence. FDGS also stresses the importance of product education and training so that all members of the team are aware not only of the current product offering, but of its history and the future of the products they support.
- **The Software Engineering Institute (SEI):** The Capability Maturity Model Integration (CMMI) developed by SEI provides a mechanism for assessing our software development process against industry best practices and offers a framework to enable FDGS to improve its software development and management capabilities. The focus is on achieving well-defined, repeatable processes. CMMI process improvement strategies are achieved by determining current process maturity, identifying the issues most critical to quality, implementing rigorous processes and metrics, and having all staff thoroughly trained.
- **Government Center of Excellence:** The FDGS team understands the nature and scope of this EVV project. Based on its experience, FDGS has formulated a knowledge center of best practices, project management methods, tools and techniques, lessons learned, and sample deliverables from our previous projects. This knowledge center, called the Government Center of Excellence, is a collection of methodologies and tools that the AuthentiCare delivery team uses to incorporate testing and quality management in all phases. This knowledge base, coupled with our experienced staff, provides the Department with an approach that adds immediate value to the EVV project.
- **Goal of Identifying Defects/Issues:** Identification of issues is not limited to development or quality assurance testing. All stakeholders are encouraged to identify defects and issues during all phases of the project. All projects encounter issues at some point, so it is important for all parties to raise issues early. This allows us to track and resolve issues in a timely manner and reduces the chance of those issues becoming major project risks.

Throughout the FDGS Quality Assurance testing task, we record any issues in the Rational Collaborative Lifecycle Management System (CLM) that FDGS uses for issue logging and tracking. The issue is recorded with the details on how to recreate the issue, along with the issue type and severity.

Any issues uncovered during an internal FDGS document and/or design deliverable review are shown in a new version of the document with track changes on. The entire EVV Project Team works in SharePoint to maintain version control.

The FDGS Quality Assurance testers track issues in the project issues tracking system. The issues are tracked in CLM from the creation of the issue, and updated during retest, resolution, and closure.

FDGS Defect tracking system will include, at a minimum, the following elements:

- **Defect #:** A unique number related to the reported issue
- **Defect Description:** A detailed description of the issue reported
- **Defect Type:** The type of issue that has been identified
- **Identified By:** The name of the person/people who identified the issue
- **Date Identified:** When the issue was identified
- **Test Environments:** Development, QA, Customer Acceptance Testing (CAT)
- **Application Type:** Web, IVR, Mobile
- **Severity:** Degree of impact a defect has on the application

After the issues have been identified, the Project Manager will work with the various teams to determine who has ownership of the issues and track the status and resolution of each issue. Those elements include:

- **Assigned To:** Name of person the issue is assigned to
- **Priority:** A value indicating the relative importance of the issue (P1: Resolve Immediately; P2: Give High Attention; P3: Normal Queue; P4: Low Priority) so the issue can be prioritized based on score
- **Severity:** The impact of the issue to the system (1: Critical; 2: High; 3: Medium; 4: Low)
- **Status:** The status of the issue as it is tracked
- **Target Resolution Date:** The expected date for remediation of the issue
- **Retest Date:** The date the defect was retested
- **Resolved Date:** The date the issue was actually resolved
- **Closed Date:** The date the issue was closed
- **Resolution Description:** A detailed description of the steps taken to resolve the issue

FDGS leverages its subject matter experts during any issue resolution to assist in the identification and mitigation of risk and share the risks and resolutions as needed in status meetings with the Department. Critical and high-severity issues—or any issues that pose a risk to the project budget and timeline—are tracked closely and reported to DHHR leadership regularly. From the creation of the RTM during requirements validation through UAT signoff, all requirements, defects, and remediation are tracked in an industry standard tool suite to verify traceability of each defect or issue to the respective requirement.

Regular status updates include tracking any defects or issues as they arise with updates as well as an Action Item Listing with updates to track outstanding action items. During implementation and throughout the life of the contract post go-live, tickets will be issued and communicated when any defects or issues are identified to provide transparency from identification through to remediation and resolution.

2.7 Change Management
2.7.1 The Vendor's proposal should describe the Vendor's approach for change management including, but not limited to methodologies, tools, and processes required to appropriately manage and document changes to the system (including, but not limited to: impact analysis, change requests)

Change Management

As described in 4.2.14 Change Management Plan of our abridged PMP, the purpose of the Change Management Plan is to confirm that any changes occurring within the project are promptly identified, coordinated, sized, agreed upon, and properly managed. FDGS understands that change is inevitable in any project of this size. In an effort to verify that changes will not have a negative impact on project success, in terms of scheduled completion, budgetary constraints, quality, or customer satisfaction, changes to plans should be expected and addressed systematically. The Change Management Plan encompasses modifications to any of the following key areas:

- **Scope**: Agreed-upon features and functions of a product or service being produced by the project, and all related requirements and deliverables
- **Project Work Plan/Schedule**: Including the Project Work Plan, planned task sequencing, task start and end dates, resource plan, baseline schedule, and baseline costs
- **Project Management Plans**: Including the resource plan, communication, risk, and issue management plans, quality management plan, and change management plan
- **Issues**: Process developed to monitor and manage issues since issues have the potential to become changes

FDGS focuses on an approach that identifies changes that could benefit the project. FDGS will also work to identify neutral changes, including "trade-offs" or exchanging one item for another.

Given the importance and visibility of the EVV project, it is imperative that executive leadership, including Department sponsors, take an active role in the change process. FDGS assumes that the Department sponsors will be the approval authority for formal changes to the EVV project. FDGS and the Department will collaborate to determine which project participants should be involved for different types of changes.

FDGS assumes that when changes affect the project schedule, cause an increase in the project budget, or require change orders/contract amendments, Department sponsors will want to be more engaged in the process. When changes do not affect the schedule, budget, scope, or contracts, FDGS assumes that our team will assume primary responsibility for addressing and implementing such changes.

2.8 Organizational Change Management
2.8.1 The Vendor's proposal should describe the Vendor's methodology, tools, and techniques for communicating and accomplishing organizational change management for DHHR. Discuss how the Vendor can assist DHHR in communicating, training, and implementing organizational change to DHHR.
2.8.2 The Vendor's proposed methodology should at a minimum address the following areas:
2.8.2.1 The Vendor's organizational change management methodology

2.8.2.2	*Determination of the impact of change*
2.8.2.3	*Methods of responding to the change, process harmonization, and approach towards potential resistance*
2.8.2.4	*Methods for helping to promote successful change management*
2.8.2.5	*Lessons Learned regarding change management challenges*

Organizational Change Management

With Electronic Visit Verification policy and requirements, we do not see many adoption issues related to organizational change management. Our focus remains on outreach to the user community, clear communication, and thorough training for administration and use of our AuthentiCare EVV solution across the entire user community.

Our Communication Management Plan complements the Outreach and Training Plan to provide all end users a clear understanding of the upcoming changes and comfort in using the intuitive web, mobile, or IVR options of the AuthentiCare EVV solution. Our team also collaborates with the Department to align outreach and communication with Department goals and timelines.

FDGS will identify and include key stakeholders in our communication and meetings where appropriate to gain buy-in and alleviate concerns that are normal with any change. We have found that combining our communication plan with our approach to training and outreach, AuthentiCare projects do not receive the pushback or resistance that other IT projects may see. Ease of use and multiple training methods allow the various end users to easily adopt the use of AuthentiCare in the field and in the office.

With AuthentiCare and our experienced delivery team from our other implementation projects, the Department gains the knowledge from lessons learned and the mitigation approach used to manage adoption and related organizational change challenges.

This next sub-section describes our Project Management Methodology (PMM). FDGS provides additional detail in this sub-section to meet the mandatory requirements listed in Table 8.1 as part of RFP Attachment 6 – Mandatory Requirements.

Table 8.1 – AuthentiCare meets all mandatory requirements for Project Management

Met	Req ID #	Requirement Text
☑	**MR002**	The Vendor must agree to adhere to the performance measures and penalties outlined within the service level agreements (SLAs) included in the request for proposal (RFP).
☑	**MR015**	The solution must be accessible for individuals with physical disabilities and vision impairments and satisfy the accessibility requirements of Section 508 of the Rehabilitation Act and the Americans with Disabilities Act (ADA).

AuthentiCare is committeed to meeting the performance measure SLAs as outlined in the RFP.

AuthentiCare is able to demonstrate substantial W3C compliance as required and the capability to use screen-reading software, like JAWS® or ZoomText®. With regard to accessibility standards, FDGS has engaged a third-party company to advise us on accessibility and use with assistive technology for the AuthentiCare Web and Mobile App. The third-party advisor has provided third-party ADA Section 508 certification of both the AuthentiCare Web and Mobile applications.

FDGS provides additional detail to the Project Management Subject Matter Area requirements in Table 8.2.

Table 8.2 – Detailed Response to Project Management Requirements

Req. ID #	Requirement Text	Requirement Type
PM001	The solution should have the ability to modify settings through the approved Change Management Plan to configure the business rules engine performing tasks, including, but not limited to:	Project Management
PM002	Rule deletion	Project Management
PM003	Rule modification	Project Management
PM004	Addition of new rules	Project Management
PM005	Business edits	Project Management
PM006	Others as defined by the Department	Project Management

The Change Management Plan confirms that any changes occurring within the project are promptly identified, coordinated, and agreed upon, and properly managed. FDGS understands that change is inevitable in any project of this size. In an effort to verify that changes will not have a negative impact on project success, in terms of scheduled completion, budgetary constraints, quality, or customer satisfaction; changes to plans should be expected and addressed in a systematic manner. The Change Management Plan encompasses modifications to any of the following key areas:

- **Scope**: Agreed-upon features and functions of a product or service being produced by the project, and all related requirements and deliverables
- **Project Work Plan/Schedule**: Including the Project Work Plan, planned task sequencing, task start and end dates, resource plan, baseline schedule and baseline costs
- **Project Management Plans**: Including the resource plan, communication, risk, and issue management plans, quality management plan, and change management plan
- **Issues**: Process developed to monitor and manage issues since issues have the potential to become changes

We know that the Department and its provider community will request future changes that cannot be known until they have worked with AuthentiCare directly. We will work with the Department to properly analyze those future change requests defined by the Department later in the implementation project or post-implementation (M&O).

PM007	The Vendor should collaborate with the Department to establish the initial roles and level of access and responsibility for each class of user.	Project Management

AuthentiCare will facilitate joint review of RFP requirements with DHHR and designated business and policy stakeholders, resulting in an approved baseline EVV Solution Requirements Traceability Matrix (RTM). During the joint review of the requirements, FDGS will demo the EVV solution to show how it satisfies the requirements, identify configurable features and functions, and identify any gaps in the EVV solution.

Using the RTM, we hold iterative requirements gathering and validation sessions (formally referred to as Joint Application Configuration [JAC] sessions) to clarify and detail the components of the current System Integration Plan (SIP) and business rules of the West Virginia DHHR AuthentiCare solution to meet the approved requirements. The FDGS Team will update the West Virginia AuthentiCare System Documentation inclusive of roles and access levels based on the design sessions and the required business rules. Following the design sessions, we will update the RTM, SIP, and AuthentiCare System Documentation based on specific requirements, and provide these items to DHHR for review and acceptance.

PM008	The solution and supporting processes should comply with the Centers for Medicare & Medicaid Services (CMS) Seven Conditions and Standards and the most current version of CMS Medicaid Information Technology Architecture (MITA). (Reference: https://www.medicaid.gov/Medicaid-CHIP-Program-Information/By-Topics/Data-and-Systems/Downloads/EFR-Seven-Conditions-and-Standards.pdf)	Project Management

AuthentiCare's integration capabilities are based entirely on open-systems standards and accommodate communications to database management systems and back-end solutions through APIs and custom imports and exports. Additional features, such as EDI 837 file creation, are built into the AuthentiCare solution and leverage the open standard architecture. AuthentiCare's feature-rich solution supports MITA's seven conditions and standards, as shown below.

Req. ID #	Requirement Text	Requirement Type

Modularity Standard

FDGS employs a modular, flexible approach to systems development, including the use of open interfaces and exposed application programming interfaces (APIs) to separate business rules from core programming. This also makes business rules available in formats that both humans and machines can read. Most business rules in AuthentiCare are captured in metadata tables in the database so that they are easily changed and updated as business rules change. The core programs in AuthentiCare use business rules that are dynamically data-driven by values in meta-tables. This separates the core functions from a specific client's setup and business rules. This meets the modularity standard's requirement to separate APIs, business rules, and core code into modules.

MITA Condition

FDGS uses the MITA conditions and standards for the development and deployment of the AuthentiCare EVV solution. We have a strong understanding of MITA and its emerging industry changes. Our knowledge of MITA and MMIS systems will benefit DHHR in potential projects involving health care information technology and the migration to its MMIS platform.

Industry Standards Condition

The AuthentiCare solution architecture and design applies industry standards whenever applicable industry standards exist. This makes the solution highly modular, extensible, interoperable, and flexible.

FDGS understands the necessity of protecting the privacy and confidentiality of your data. The AuthentiCare solution provides world-class security thanks to Fiserv's global security practices and procedures. The EVV system meets the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA-compliant practices include:

- Data transfers employ AES 256-bit encryption and TLS 1.2 or SFTP
- Users are individually registered and functional rights and roles are assigned to their login credentials
- Both IVR and Mobile App employ two-factor authentications as required
- Users are data scoped to see only relevant data that they are allowed to see
- ANSI X-12 transactions are employed where relevant

With regard to accessibility standards, FDGS has engaged Level Access to advise us as to accessibility and use with assistive technology for the AuthentiCare Web and Mobile App. Level Access has provided third-party ADA Section 508 certification of both the Web and Mobile applications.

Leverage Condition

The AuthentiCare solution is inherently a Software-as-a-Service (SaaS) solution and the interfaces to use it are sharable and reusable within West Virginia agencies. In particular, the Mobile App supports multiple configurations with different business rules. The business rules set is selected by a configuration code, while user preferences are applied when the user logs in. This is achieved with only one common app each in the Apple App Store and Google Play.

The AuthentiCare solution is in full production in several states, with each state having the solution modules relevant to their specific business and program needs.

Business Results Condition

The AuthentiCare solution is a modular, flexible, extensible, interoperable, service oriented architecture (SOA)-based system that provides near real-time EVV data. This supports accurate and timely claims processing and effective communication for all DHHR users, providers, applicants, beneficiaries, and plans. MMIS claim payment rates are typically in excess of 99 percent, so providers have few denied claims, reducing rework for both providers and agency staff. By only allowing billing for documented services delivered, states typically see a 5 – 12 percent spending reduction by not paying for missed or shortened visits. The best providers have a renewed focus on quality of care and providing all of the services beneficiaries are supposed to receive.

Reporting Condition

AuthentiCare comes with a robust web and reporting solution that provides information to support program evaluation, continuous improvement in business operations, transparency, and accountability. Ad hoc queries provide management with additional reporting capabilities.

Interoperability Condition

Req. ID #	Requirement Text	Requirement Type
The AuthentiCare EVV solution architecture is based on a Service Oriented Architecture (SOA), and these services are available for other customer-approved system consumption external to EVV. FDGS adopted SOA to meet our customers' current and future business requirements and to meet security, scalability, reliability, and availability requirements. The SOA architecture will be beneficial for DHHR using the AuthentiCare integration with its MMIS platform. The AuthentiCare solution can be integrated into a larger SOA architecture using data interfaces and application programming interfaces (API) and accessed by any Medicaid enterprise application in need of our services. AuthentiCare solution processes employ data interchange and web service standards including secure JSON API and restful (REST) web services. This API infrastructure has been proven in production operations for over five years. Our solution processes employ Security Standards including TLS 1.2 Transport Level Security protocol, SFTP protocol for managed file transfers, and certificate authentication for file transfer portals. AES 256-bit encryption, together with these protocols, meets the secure standards required for exchange of PHI under HIPAA.		
PM009	The Vendor should conduct an overview with the Department of solution changes that are ready to be moved into the production environment as directed in the Change Management Plan.	Project Management
The AuthentiCare team follows standard change management processes, which includes communication in advance of post-production maintenance and release details. Pre-production changes follow standard implementation processes.		
PM010	The Vendor should request authorization in writing from the Department prior to promoting any system changes to the production environment or solution as agreed upon by the department.	Project Management
The FDGS team agrees to provide a clear schedule of patching dates and product releases in advance of future system changes. For example, the 2020 patches to AuthentiCare are already planned for the third Saturday of each month, and planned production code release events for 2020 are scheduled quarterly at the end of the month between the hours of 7 PM on Wednesday through 3 AM Central on Thursday. Future schedules of ongoing patches and product releases will be communicated to the Department well in advance of the next promotion date. In some instances, major vulnerabilities must be completed in an expedited fashion to close the risk. FDGS will notify the Department following emergency patches and promotion to production.		
PM011	The solution should have the ability to allow the modification of edits per the Change Management Plan.	Project Management
The AuthentiCare solution shall have the ability to be modified per the Change Management Plan if both the Department and FDGS team agree to the changes, alterations in timeline and any additional cost that may be incurred.		
PM012	The Vendor should provide a manual visit verification process that is adaptable to changes in program requirements throughout the contract period as directed by the Change Management Plan.	Project Management
AuthentiCare provides the ability to modify verification data and all modifications will be logged and maintained. In addition, AuthentiCare provides a manual visit verification process for DHHR when electronic visit verification is unavailable. FDGS has found that these manual scenarios are rarely necessary when using our AuthentiCare solution. We include exception reporting for claims that do not have both an electronic check-in and check-out. If necessary, the user may upload copies of paper timesheets and other electronic document files. The AuthentiCare website provides an easy-to-use interface for providers to document service and create web visits when manual verification is required. The process includes additional scrutiny that we have found useful based on our experience in other states, like requiring the provider to select from a list of acceptable reasons and then detail the event in notes. Some states go further, requiring web-created visits to be reviewed and either approved or rejected by the MCO. These additional requirements have led to a significant reduction in web-based claims. For manual verification, the AuthentiCare web provides pages to create a single visit claim or an express claims process for rapid entry from a paper timesheet or notes. The AuthentiCare EVV system provides robust auditing for both electronic and manual entry. Manual visit entry stores information entered including who initiated/created the claim, the billing provider, member, worker, date/time of visit, reason for manual verification, and the date/time the claim was created. Additionally, member/family member attestation can be obtained for manual visit verification claims. To control the number of manual exceptions, instead of the more efficient electronic options, AuthentiCare provides configurable controls and exception reporting to identify DCWs that may have excessive manual verifications. Drill down to history records for claims (visit data) and for authorizations are available to state administrators, MCOs, and providers to support research and exception processing.		

Req. ID #	Requirement Text	Requirement Type
The AuthentiCare EVV system is accustomed to accommodating changes in program requirements, whether for services, claims processing rules, or manual visit verification. When appropriate, AuthentiCare can be configured to require providers to attest to hard copy documentation for manual visit verification claims. While manual visit verification will be the exception, our AuthentiCare solution provides DHHR the critical flexibility with configurable options and parameters to manage manual visit verification processes according to policy and procedures.		
PM013	The solution reporting should be configurable so that standard reports and recipients of reports can be changed easily over the life of the contract without additional cost, as defined in the approved Change Management Plan.	Project Management
FDGS will work with DHHR to set the appropriate access to all reporting features and functions based on the user role. For example, a "Scheduler Coordinator" role could be limited to specific scheduling functions and reports related to scheduling like the Calendar and Late and Missed Visits Reports. Another scenario within our AuthentiCare solution allows all web users to set report content and run reports in real-time or on a schedule, but only reports and content for which their user role gives access. FDGS will work with DHHR to establish role-based access to the reporting function. As an example, a common standard provider role is the "Administrator" or "Admin Assistant," which has access to all reports. Other standard roles like "Human Resources'" would be limited to worker-related reports. This information will be included in the AuthentiCare Reporting User Guide. As DHHR continues to use AuthentiCare and determines changes to the roles and access are necessary, FDGS will support the Department with the appropriate configuration updates. AuthentiCare allows DHHR staff to simply configure system changes on their own to adjust roles and access as policies and procedures are updated. Details for user roles and access to the AuthentiCare functions are documented in the West Virginia DHHR AuthentiCare User Guide for easy reference.		
PM014	The Vendor should update the user manual and receive Department approval each time a solution change or upgrade is implemented as directed by the Change Management Plan and within an agreed upon time-frame by the Department.	Project Management
FDGS agrees to submit the updated user manual and related documentation to the Department for review and approval prior to implementation of changes or upgrades completed as part of the Change Management Plan. Depending on the extent of the changes in a release, FDGS will work with the Department to agree on the lead time necessary to complete its review. The training materials in the AuthentiCare User Manual will be tailored for West Virginia EVV programs. This is a comprehensive user manual that documents and explains system functionality. The advantage is that this is an organic document, regularly updated and accessible and searchable online, that reflects changes and enhancements to AuthentiCare functionality. West Virginia's AuthentiCare User Manual will be updated to reflect enhancements and other system updates identified during the iterative Design Sessions as well as future planned releases.		
PM015	The Vendor should provide updates to the user manual and have the updated manual available to users no later than thirty (30) days prior to the date a solution change is implemented as directed by the Change Management Plan.	Project Management
FDGS' Training Lead will provide West Virginia DHHR written details and updated procedures to any new functionality that impacts users prior to being moved to production. In general, the AuthentiCare user manual is updated at least annually and with significant product upgrades. For less significant releases, the AuthentiCare release notes appropriately document the changes. We will share these artifacts with DHHR 30 days prior to the functionality's release.		
PM016	The Vendor should configure the solution for specific Medicaid waivers/services at no additional cost to the Department, per the Change Management Plan.	Project Management
AuthentiCare will be configured at the time of the final design for the current Medicaid waivers/services in place with West Virginia. If additional waivers/services are instituted or required after implementation, a change order would need to be submitted to the Account Manager.		
PM017	The solution should have the ability to support data integrity through system controls for software program changes and promotion to production as defined in the approved Change Management Plan.	Project Management
AuthentiCare maintains data integrity through a strategy of controls incorporating audit, access, security and policies. We provide a documented change management process to control the transfer of software between the development,		

Req. ID #	Requirement Text	Requirement Type
test, and production environments. Multiple approvals are required including review from our change management team. Change requests must be sanctioned or fully approved at a minimum of 24 business hours or escalated approvals are required. All changed are assigned a risk level and each record requires a detailed implementation, validation and back-out plan.		
PM018	The solution should support workflow development by the vendor based on new processes defined by the Department according to business needs as identified in the Change Management Plan.	Project Management
Customizations of work flows and other requirements follow the design process leveraging the RTM and SIP or following the standard Change Management process.		
PM019	The solution should have the ability for the Department to control and monitor system change requests as defined in the approved Change Management Plan.	Project Management
The project Change Log, defined in the Change Management Plan, is used to control and monitor system change requests managed throughout the life of the project. System change requests, the change request log, and associated details including status are maintained outside of the AuthentiCare application as part of our project management controls. The approved Change Management Plan will document the location of the change requests, log, and related materials. The FDGS Project Manager will provide status on change requests as required for all project status reports.		
PM020	The solution should have the ability for the Department to set and change priority levels on individual change requests as defined in the approved Change Management Plan.	Project Management
AuthentiCare will work with DHHR on prioritizing change requests based on the collaboratively agreed-upon Change Management Plan.		
PM021	The Vendor should conduct a security, privacy, and/or risk assessment of any new functionality prior to its deployment to production , the results of which should be delivered to the Department within an agreed upon timeframe by the Department. The Vendor should obtain Department approval for proposed resolutions to all assessment findings prior to deployment to production per the Change Management Plan.	Project Management
This is a requirement of the CMS Outcomes Based Certification (OBC) Operational Readiness Review (ORR) to provide a summary NIST 800-30 v1 independent audit report. FDGS agrees to conduct the security, privacy, and/or risk assessment of any new functionality prior to its deployment to production. We will provide the results of assessments to the Department within an agreed upon timeframe.		
PM022	The Vendor should coordinate all testing activities as agreed upon by the Department.	Project Management
Testing consists of promoting the configured system through: • Quality Assurance Test environment for FDGS quality assurance testing • Client Acceptance Test environment for User Acceptance Testing Deployment results in a request for the customer to sign off that the application is ready for FDGS to migrate the overall solution into production. Our teams provide iterative system testing through our Quality Management and Testing approach as well as User Acceptance Testing by the AuthentiCare team and DHHR. FDGS follows a disciplined Quality Assurance (QA) approach that contributes to our record of delivering projects on time, within budget, and with high quality. This Structured Test Methodology (STM) verifies that all functional and system-wide requirements are complete and confirms the configuration requirements. In support of the STM, AuthentiCare has a dedicated team of testing subject matter experts that comprise our Testing Center of Excellence (TCoE) pool of resources. The TCoE pool of resources is equipped with the processes, technology, tools, infrastructure, and talent to support quality deliverables. The project team will work closely with TCoE pool of resources to provide the highest level of quality assurance throughout the entire lifecycle of the project. The quality assurance management processes and controls that our teams use are documented in the overall TCoE testing process and UAT process.		
PM023	The Vendor should prepare a comprehensive set of test scenarios, within a timeframe as agreed upon by the Department, including but not limited to:	Project Management

Req. ID #	Requirement Text	Requirement Type
PM024	Applicable test cases	Project Management
PM025	Expected test results	Project Management
PM026	Others as defined by the Department	Project Management
Test plans and scripts will be shared and reviewed with the Department.		
PM027	The Vendor should provide the Department and/or its designees access to test cases and test data to facilitate execution of applicable testing cycles.	Project Management
Test cases and test data are created by the TCoE pool of resources to facilitate execution of applicable testing cycles and provided to the Department.		
PM028	The Vendor should provide the Department with a fully tested and operations-ready User Acceptance Test environment that is isolated and separate from all other environments.	Project Management
FDGS teams maintain a Development and Quality Assurance (QA) environment for our configuration and testing activities. Future enhancements and ongoing maintenance activities will be applied to these regions and tested prior to promoting the updates to the next environment for User Acceptance Testing (UAT) by DHHR. We will establish and maintain the Client Acceptance Test (CAT) environment to conduct the initial and future User Acceptance Testing. The CAT environment is also used for Training DHHR staff, provider agencies, and other end users. FDGS' Software Development Life Cycle (SDLC) calls for promotion of applications across separate, isolated environments beginning in our Development environment, followed by QA, CAT/UAT, and finally, Production, which includes Disaster Recovery (DR) in a geographically diverse location. These environments exist on different virtual servers with Development and Production in Chandler, Arizona, and QA, CAT, and DR in Omaha, Nebraska.		
PM029	The Vendor should discuss and finalize with the Department the level of testing required based on the significance of the change as directed in the Change Management Plan.	Project Management
The level of testing required by the significance of a change is determined through the agreed-upon Change Management Plan.		
PM030	The Vendor should provide the Department weekly reports of testing status, including, but not limited to:	Project Management
PM031	Metrics on the number of tests completed	Project Management
PM032	Number of deferred or canceled tests	Project Management
PM033	Results of the tests executed	Project Management
PM034	Defects identified by severity level	Project Management
PM035	Corrective actions taken	Project Management
PM036	Others as defined by the Department	Project Management
AuthentiCare will provide testing status reports as defined and agreed upon in the Testing Plan.		
PM037	The Vendor should conduct Pilot Testing to validate the capacity and processing capabilities of the solution in a tightly controlled production environment.	Project Management
AuthentiCare has conducted pilot phases in many implementations and will work with DHHR to determine the timing of pilot phase milestones and deliverables.		
PM038	The Vendor should include a test of actual data processing in a full operational environment, with successful end-to-end solution functionality during Pilot Testing.	Project Management

Req. ID #	Requirement Text	Requirement Type
AuthentiCare has the ability to do end-to-end testing in the Client Acceptance Testing environment. Validation of the same end-to-end functionality is repeated in the production pilot test.		
PM039	The Vendor should provide written test results of the Pilot Testing to the Department within an agreed upon timeframe.	Project Management
Test deliverables will align to the agreed upon Testing Plan.		
PM040	The Vendor should provide the Department official written notification of readiness for full production operations after completion of Pilot Testing.	Project Management
The AuthentiCare project team will provide written notification of operational readiness and completion of testing at the agreed-upon milestone for pilot testing.		
PM041	The Vendor should work with the Department to develop an interface testing acceptance standard to outline the minimum requirements that must be met prior to allowing external electronic visit verification (EVV) data partners to submit data to the EVV solution.	Project Management
Prior to releasing the application into production, DHHR staff will participate in a cycle of UAT. In this phase, a group that represents a cross-section of end users tests the application. UAT is performed using real-world scenarios that are relevant to end users in the Client Acceptance Test (CAT) environment. The CAT environment will contain the appropriate test data as well as converted data necessary to verify any required conversion processes. During this phase, end-to-end interface testing is also performed in the CAT environment. FDGS will work with DHHR to develop detailed test scenarios and standards to support UAT. These detailed test scenarios will allow DHHR to test all functional aspects of the system and confirm performance in accordance with the specifications. Our project and technical teams will provide support throughout this process, which includes answering questions, researching issues, executing corrections, and retesting software components. FDGS and DHHR have equally important roles in the confirmation and acceptance of the final system prior to production release. It is critical that testing scenarios receive the proper level of attention from all parties early in the product life cycle. FDGS' experienced team of implementation specialists will work with the Department's team to develop a sample of test scenarios to support this project phase. Once the Department is satisfied that the application is producing the expected results, FDGS will initiate the final production implementation tasks.		
PM042	The Vendor should conduct interface testing with external electronic visit verification (EVV) data partners approved by the Department.	Project Management
AuthentiCare will work with DHHR to develop pilot interface acceptance criteria and identify the approved data partners to conduct interface testing.		
PM043	The Vendor should provide testing and training environments that include sufficient, representative data elements that are in the production environment. The Vendor should not invoke or charge the Department for license fees for any of the testing or training environments.	Project Management
FDGS will establish and maintain the Client Acceptance Test (CAT) environment in the same secure data center as our production and disaster recovery environments. The CAT environment is secured behind our firewalls within our enterprise-level data centers with full back-up and recovery procedures. The CAT environment is fully scalable up to the same specifications and volumes of production, if needed. Data elements are representative of production allowing for complete usability in User Acceptance Testing. Testing vendor staff and assigned DHHR staff will have access to the CAT environment to execute UAT. FDGS will work with the Department to develop detailed test scenarios to support UAT. These detailed test scenarios will allow DHHR to test all functional aspects of the system and confirm performance in accordance with the specifications and the approved RTM. Our project and technical teams will provide support throughout this process, which includes answering questions, researching issues, executing corrections, and retesting software components. The CAT environment serves as the environment for both initial and ongoing training to DHHR staff. The AuthentiCare CAT environment is updated prior to approved enhancements and future product releases are applied to the production version so that the CAT/UAT and training environment remains current.		
PM044	The Vendor should use a User Acceptance Testing (UAT) environment that mirrors all programs in production to allow the Department to conduct testing prior to new software updates and to serve as an ongoing training platform for users.	Project Management

Req. ID #	Requirement Text	Requirement Type
We maintain the Client Acceptance Test (CAT) environment to conduct the initial and future User Acceptance Testing. The CAT environment is also used for training staff, provider agencies, and other end users. This environment is in the same secure data center as our production and disaster recovery environments. The CAT environment is secured behind our firewalls within our enterprise-level data centers with full back-up and recovery procedures. The CAT environment is fully scalable up to the same specifications and volumes of production, if needed. Testing vendor staff and assigned DHHR staff will have access to the CAT environment to execute UAT prior to code deployments. FDGS will work with the Department to develop detailed test scenarios to support UAT. These detailed test scenarios will allow DHHR to test all functional aspects of the system and confirm performance in accordance with the specifications and the approved RTM.		
PM045	The Vendor should create, use, and make available to the Department, representative samples for testing edits, business rules, and workflow processing.	Project Management
Test edits, business rules, workflow samples, and documentation will be provided as defined in the Testing Plan.		
PM046	The Vendor should create or modify existing data as needed for testing in a test environment, in compliance with federal guidelines. (Reference: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Downloads/TestingFramework.pdf)	Project Management
FDGS will populate the test environments with created and modified data to execute the test plans and scenarios necessary to validate the correct functionality. We do not allow production data into test environments that may expose PHI or PII to unauthorized access.		
PM047	The Vendor should maintain a clearly organized test case library that can be accessed by all testers, including Department users, with search capability that is cross-referenced to the code that it tests.	Project Management
AuthentiCare testing team creates a test library made up of Test Scenarios and Test Cases. AuthentiCare will assist in test scenario and case management for UAT testers including Department users that is cross referenced to the requirements that it tests.		
PM048	The Vendor should ensure web portal design, development, implementation (DDI) and operations are in accordance with Department and federal regulations and guidelines related to security, accessibility, confidentiality, and auditing. (Reference: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/IS_Policy-.pdf)	Project Management
The Product Specialists focus on the detailed workings of AuthentiCare and the components supporting the various user interface platforms. They also are critical to tasks and activities supporting the product and its future roadmap including: • Evaluation of new policy, guidelines, and requirements at the federal level (CMS) • Reviews and consideration of feedback and product enhancement requests from the AuthentiCare customer base • Collaboration with product ownership to define and support the AuthentiCare product roadmap for future enhancements Additional help desk and operational support including troubleshooting, root cause analysis, and problem resolution. The Certification SME will support AuthentiCare requirements definition and project activities from Project Initiation through to formal certification by CMS including: • Review any applicable CMS updates to the Certification process • Participate in Requirements Validation and design/configuration sessions identifying requirements specific to CMS Certification • Work with Business Analyst and Test Analyst on scenarios for business function CMS requirements and test case development • Review test cases and results for the CMS certification scenarios and validation • Support Training & Outreach in areas such as HIPAA awareness training materials in the various user role training • Identify and support the gathering of all required evidence for CMS Certification		
PM049	The solution should be developed and implemented in accordance with the project work plan.	Project Management
At the start of the West Virginia EVV project, the abridged project schedule included in this response will be expanded by the FDGS Project Manager and reviewed with relevant stakeholders. FDGS understands that the project work plan is subject to input and final approval by DHHR.		

Req. ID #	Requirement Text	Requirement Type
PM050	The Vendor should conduct the following types of testing in support of the solution:	Project Management
PM051	Unit testing	Project Management
PM052	Iterative functional testing	Project Management
PM053	System integration testing (SIT)	Project Management
PM054	Interface testing	Project Management
PM055	Regression testing	Project Management
PM056	End-to-end testing	Project Management
PM057	Security testing	Project Management
PM058	Performance testing	Project Management
PM059	Usability/Accessibility testing	Project Management
PM060	Browser testing	Project Management
PM061	User acceptance testing (UAT)	Project Management
PM062	Data conversion testing	Project Management
PM063	Operational readiness testing (ORT)	Project Management
PM064	Other testing as identified by the Department and/or Vendor	Project Management

Our test strategy and plan focuses on the benefit of using a mature SaaS EVV solution. As configuration is completed to support the West Virginia EVV program and policies, we conduct multiple levels of testing to verify that unexpected errors are not introduced as well as regression testing to confirm known functions act appropriately.

Also, with our iterative design approach, we are able to complete the testing cycles and then demonstrate the added functionality from each contract milestone to the Department.

Unit Testing

Our development staff will execute unit tests to confirm that any code changes and configuration modifications meet design requirements and behave as intended.

Iterative Functional Testing

FDGS follows a disciplined Quality Assurance (QA) approach that contributes to our record of delivering projects on time, within budget, and with high quality. This Structured Test Methodology (STM) verifies that all functional and system-wide requirements are complete in each iteration and confirms the configuration requirements.

Our team uses quality assurance management processes and controls, which are documented in the overall TCoE testing process. The testing approach, objectives, schedule, and procedures are documented in our test plan along with phase entrance and exit criteria.

System Integration Testing (SIT)

The QA Team designs, builds, and executes test scripts so that application features are confirmed throughout configuration change management activities. Testing results conducted by the FDGS testing team will be documented and summarized for DHHR to review as part of the System Integration Testing deliverable. FDGS will submit SIT test results to DHHR for approval prior to the migration to UAT.

Req. ID #	Requirement Text	Requirement Type

Interface Testing

FDGS works with system components and its respective vendors to conduct interface testing for AuthentiCare. Our teams are experienced in working with various states and their vendors to successfully complete interface testing and verification of accurate data exchange. West Virginia systems can interface with AuthentiCare through the latest industry-standard specification (JSON/REST) web service transactions or, as an alternative, the standard XML file Application Programmer Interface (APIs) hosted by FDGS. Besides our other statewide integration projects, FDGS has successfully designed and implemented multiple file exchanges with vendors including DXC, United Healthcare (UHC), BlueCross BlueShield, Presbyterian Health Plan, Molina Healthcare, MediWare Information Systems, and various state Medicaid systems and clearinghouses.

Regression Testing

The QA Team designs, builds, and executes regression test scripts so that application features are confirmed throughout configuration change management activities. For every software modification introduced, a regression test cycle is performed to protect the integrity of the system code set. Future software modifications result in additions to the regression test deck and become part of the comprehensive test package used to confirm release and change management activities.

End-to-end Testing

FDGS establishes System Test (QA) and Customer Acceptance Test (CAT) environments in the same data center as our production AuthentiCare solution. All test environments are scalable, if necessary, to mirror that capacity of the production environment. The test environments are of adequate size for performance testing. End-to-end testing using test data are available through the CAT environment.

Security Testing

Penetration testing is conducted to comply with FDGS policy, customer mandates, and Payment Card Industry Data Security Standard (PCI-DSS) requirements. The purpose of penetration testing is to measure the security posture of a target system or environment. Penetration testing is not simple hacking but, instead, is a process designed to validate security weaknesses, identify attack vectors, and validate the functionality of security controls. The penetration testing process FDGS uses a 'gray' box approach as defined in NIST 800-115 Technical Guide to Information Security Testing and Assessment. Penetration tests are designed to be non-destructive, and minimize the potential impact to systems or networks under test.

Performance Testing

FDGS uses its production-comparable Quality Assurance (QA) environment to complete performance and load testing activities. The technical team uses IBM Rational Performance Tester to identify system performance bottlenecks, reduce load testing, and analyze the impact of load from the different AuthentiCare application components.

Usability/Accessibility Testing

AuthentiCare uses third-party accessibility vendor for usability/accessibility testing. Documentation is available demonstrating support for 508 guidelines and WCAG 2.0 and 2.1. JAWS is used in the validation process.

Browser Testing

AuthentiCare is available to users via standard web browsers. Testing is performed in Microsoft Internet Explorer/Edge, Apple Safari, Mozilla Firefox, and Google Chrome. The current and previous version are supported. These were selected based on industry usage statistics.

User Acceptance Testing (UAT)

EVV end users and assigned DHHR staff will have access to the CAT environment to execute User Acceptance Testing (UAT). Prior to releasing the application into production, staff will participate in a cycle of UAT. In this phase, a group that represents a cross section of end users tests the application. UAT is performed using real-world scenarios that are relevant to end users in the Client Acceptance Test (CAT) environment. During this phase, end-to-end interface testing is also performed in the CAT environment.

FDGS will work with the Department to develop detailed test scenarios to support UAT. These detailed test scenarios will allow DHHR to test all functional aspects of the system and confirm performance in accordance with the specifications and the approved RTM. Our project and technical teams will provide support throughout this process,

Req. ID #	Requirement Text	Requirement Type

which includes answering questions, researching issues, executing corrections, and retesting software components.

FDGS and DHHR have equally important roles in the confirmation and acceptance of the final system prior to production release. It is critical that testing scenarios receive the proper level of attention from all parties early in the product life cycle. FDGS' experienced team of implementation specialists will work with the Department's team to develop a sample of test scenarios to support this project phase. FDGS agrees that we meet all requirements for this section.

The FDGS technical team establishes the CAT environment used for both User Acceptance Testing (UAT) and then initial and ongoing training. The AuthentiCare CAT environment is updated prior to approved enhancements and future product releases are applied to the production version so that the CAT/UAT and training environment remains current.

Once the Department is satisfied that the application is producing the expected results, FDGS will initiate the final production implementation tasks.

Data Conversion Testing

Data Conversion Testing is crucial and will be a priority in all phases of the project to confirm that the data exchanged in the DHHR solution meets all requirements and enables all business units effected, as well as the MMIS to function appropriately. Data interchanges will be identified in the planning phase and during the development phase, all integration specifications will be designed and accepted by DHHR. Data integration must occur using file exchange through approved File Gateway methods to verify that PII/PHI security and will be thoroughly tested with all vendor partners.

Operational Readiness Testing (ORT)

FDGS initiates production readiness tasks that involve implementing the system and importing data into the production environment. FDGS' recommended approach is to conduct a soft go-live in which providers have the opportunity to validate client, provider, and worker demographic data as well as authorizations.

At this stage, the newly configured AuthentiCare solution for West Virginia is ready for full production cutover. The FDGS Team confirms that DHHR, stakeholders, your provider community, and other users have the necessary support for a smooth and successful launch of the solution.

During the agreed cutover period, the FDGS implementation team will transition the system to the FDGS Global Service Delivery for ongoing customer service support.

PM065	The Vendor should be prepared to assist the Department, as necessary, with User acceptance testing (UAT).	Project Management

Prior to releasing the application into production, DHHR staff and its testing vendor will participate in a cycle of UAT. In this phase, a group that represents a cross-section of end users test the application. UAT is performed using real-world scenarios that are relevant to end users in the Client Acceptance Test (CAT) environment. The CAT environment will contain the appropriate test data as well as converted data necessary to verify any required conversion processes. During this phase, end-to-end interface testing is also performed in the CAT environment.

FDGS will work with DHHR to develop detailed test scenarios to support UAT. These detailed test scenarios will allow DHHR to test all functional aspects of the system and confirm performance in accordance with the specifications. Our project and technical teams will provide support throughout this process, which includes answering questions, researching issues, executing corrections, and retesting software components.

FDGS and DHHR have equally important roles in the confirmation and acceptance of the final system prior to production release. It is critical that testing scenarios receive the proper level of attention from all parties early in the product life cycle. Our experienced team of implementation specialists will work with the Department's team to develop a sample of test scenarios to support this project phase.

Once the Department is satisfied that the application is producing the expected results, FDGS will initiate the final production implementation tasks.

PM066	The Vendor should be prepared to conduct User acceptance testing (UAT) in all cases whereby the Department does not elect to conduct UAT.	Project Management

In addition to a support role through UAT, as noted in PM065, FDGS is prepared to conduct UAT. However, if UAT execution is requested by the Department, the FDGS Account Manager will open discussions to identify existing issues

Req. ID #	Requirement Text	Requirement Type
prior to expanding UAT to determine if alternatives are available to maintain a support role for the AuthentiCare team. To avoid any conflict, we have found it best to remain in a support role through the UAT phase.		
PM067	The Vendor should complete regression testing subsequent to, but not limited to, the following:	Project Management
PM068	Deployment of new solution components	Project Management
PM069	Integration of each solution component into the primary solution	Project Management
PM070	Every migration of new build versions to each test environment	Project Management
PM071	Solution fixes	Project Management
PM072	Solution patches	Project Management
PM073	Solution releases	Project Management
PM074	Others as defined by the Department	Project Management
The QA Team designs, builds, and executes regression test scripts for every software modification introduced. A regression test cycle is performed to protect the integrity of the system code set. Future software modifications result in additions to the regression test deck and become part of the comprehensive test package used to confirm release and change management activities. Additionally, negative test cases are written and executed to test unexpected behavior and boundary limits of the application. All application releases are subject to stress/load testing activities that simulate heavy production cycles, to confirm that code modifications are production ready.		
PM075	The Vendor should utilize a subset of system integration testing (SIT) scenarios representative of maximum functional and technical solution coverage for the purposes of regression testing.	Project Management
The QA Team utilizes a full regression for reaching maximum functionality of the technical solution. We will work with DHHR on specific integration scenarios identified.		
PM076	The Vendor should obtain approval from the Department on which scenarios should be used for regression testing.	Project Management
The QA Team will review all regression test plans and scripts with DHHR for approval and acceptance.		
PM077	The Vendor should utilize end-to-end test cases in support of regression testing.	Project Management
The QA Team utilizes end-to-end test cases as part of regression testing and will work with DHHR during the script reviews for approval and acceptance.		
PM078	The Vendor should perform privacy and security testing on functional, technical, and infrastructure components to ensure the solution meets all State, Department, and Federal privacy and security requirements. (Reference: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/IS_Policy-.pdf)	Project Management
FDGS' Unified Vulnerability Management Services (UVMS) Team's primary responsibility is to perform periodic penetration tests and vulnerability assessments of FDGS' infrastructure and applications. UVMS plays a vital role in helping to protect customer information and the assets of FDGS. UVMS employs a variety of technologies, tools, and techniques to help make sure that high-quality security assessments are performed. Security assessments identify vulnerabilities that may represent varying degrees of risks to FDGS. Vulnerabilities deemed of risk to FDGS are assigned to appropriate individuals who are required to take action to mitigate any risks associated with identified vulnerabilities. ***Assessments*** ***Penetration Testing***: Penetration testing is conducted to comply with FDGS, customer mandates, and Payment Card		

Req. ID #	Requirement Text	Requirement Type
Industry Data Security Standard (PCI-DSS) requirements. The purpose of penetration testing is to measure the security posture of a target system or environment. Penetration testing is not simple hacking but, instead, is a process designed to validate security weaknesses, identify attack vectors, and validate the functionality of security controls. The penetration testing process FDGS uses is a 'gray' box approach as defined in NIST 800-115 Technical Guide to Information Security Testing and Assessment. Penetration tests are designed to be non-destructive, and minimize the potential impact to systems or networks under test. ***Third-Party Penetration Testing***: UVMS facilitates an annual third-party security assessment of external networks. These tests are performed in addition to UVMS testing, and are executed by an approved, independent third party. Only GCSF-approved vendors are authorized to execute testing on FDGS' behalf, in accordance with FDGS policy. ***Vulnerability Scans***: A vulnerability scan is an automated process that is designed to assess computers, computer systems, networks, or applications for security vulnerabilities or weaknesses. While functionality varies between different types of vulnerability scanners, they share a common, core purpose of enumerating the vulnerabilities present in one or more targets. In accordance with FDGS policy, UVMS uses Nessus and Trustkeeper to perform regular vulnerability scans of FDGS' network and computer systems. The scanning tools used are considered industry standard and are customized to test FDGS networks in an efficient manner, while minimizing the potential risks associated with active scanning. Vulnerabilities deemed of risk to FDGS are assigned to appropriate individuals who are required to take action to mitigate any risks associated with identified vulnerabilities. **Testing Results:** FDGS UVMS tracks and reports on results of the security assessments performed. Results of ad hoc assessments performed outside of normal testing cycles are provided to the requester, system owner, and the Cyber Risk Manager responsible for the network or system under test. **People:** UVMS personnel are required to meet minimum qualification standards. Industry and military experience, educational background, and certifications are the basis for making hiring decisions. **Governance:** The operations of UVMS are governed by FDGS' Global Cyber Security Policy and Standards. UVMS objectives encompass areas such as the frequency of vulnerability tests, the scope of the assessment, and the required outputs of the process. Objectives are reviewed annually, or as necessary when policy changes are made, to validate consistency with the Global Cyber Security Policy. **Methodologies:** UVMS has formal, documented assessment methodologies and procedures in place describing the processes and steps to be followed when performing security assessments. These documents give general information regarding the process to initiate, approve, perform, and conclude security assessments, as well as procedures for using each of the security assessment tools. **Logical and Physical Access:** Because of the sensitive nature of the tools used and procedures performed by UVMS, specific security measures have been taken to restrict access to UVMS systems. Logical access to the systems from which vulnerability assessments are performed is restricted to UVMS staff. UVMS staff must individually authenticate to each server with a public/private key pair in order to access the security assessment tools. Physical access to UVMS systems and facilities is restricted to authorized individuals only. Access to the Cyber Vulnerability Center is maintained, administered, and controlled by Corporate Security. Additionally, an electronic record is maintained by Corporate Security of access to secured areas.		
PM079	The Vendor should propose testing scenarios and/or cases to the Department for their approval.	Project Management
As part of the Testing Plan, AuthentiCare will provide a review of the testing plans for the various testing components such as SIT and UAT as well as associated testing scenarios to DHHR for review and approval.		
PM080	The Vendor's performance testing methodology should allow for performance tests to be representative of the expected peak period volumes for solution operation	Project Management
AuthentiCare uses its production-comparable Quality Assurance (QA) environment to complete performance and load testing activities. These tests are at or exceed expected peak load conditions. The technical team uses IBM Rational Performance Tester to identify system performance bottlenecks, reduce load testing, and analyze the impact of load from the different AuthentiCare application components. Testing results conducted by the FDGS testing team will be documented and summarized for DHHR to review as part of the Performance Testing deliverable. FDGS will submit test results to DHHR for approval prior to the migration to UAT.		

Req. ID #	Requirement Text	Requirement Type
PM081	The Vendor's performance testing should occur on a production ready version of the solution.	Project Management
The performance environment used for testing is a production-comparable Quality Assurance environment.		
PM082	The solution's performance testing environment should mirror the final production solution specifications.	Project Management
The AuthentiCare production-comparable Quality Assurance (QA) environment used to complete performance and load testing activities is configured to production design and build. The test scripts execute so that application features are confirmed throughout configuration management activities.		
PM083	The Vendor should perform usability/ accessibility testing for various types of users, including, but not limited to:	Project Management
PM084	Internal users	Project Management
PM085	External users	Project Management
PM086	Users with limited computer skills	Project Management
PM087	New user registration	Project Management
PM088	Users with disabilities	Project Management
PM089	Others as defined by the Department	Project Management
AuthentiCare is able to demonstrate substantial W3C compliance as required and has the capability to use screen reading software, such as JAWS® or ZoomText®. With regard to accessibility standards, FDGS has engaged Level Access to advise us as to accessibility and use with assistive technology for the AuthentiCare Web and Mobile App. Level Access has provided third-party ADA Section 508 certification of both the Web and Mobile applications. Copies of the most recent AuthentiCare VPAT reports are available upon request.		
PM090	The Vendor should conduct an Operational Readiness Review (ORR) prior to statewide implementation of the solution.	Project Management
The CMS EVV Outcomes Based Certification (OBC) process requires an Operational Readiness Review (ORR) prior to go-live for EVV implementations. With a phased implementation, the State Medicaid Agency and their CMS representative would determine the best timing for conducting the ORR prior to full production. The CMS EVV ORR requires submission of the 11 Criteria evidence and independent audit reports as defined in the OBC guidance, a minimum of two weeks prior to the scheduled CMS ORR meeting. DHHR should allow a minimum of 30 to 45 days after configuration and DDI of their AuthentiCare solution implementation to complete the required third-party security and privacy audits, prepare the certification evidence, submit the reports and evidence to CMS and to get scheduled on the CMS calendar for the ORR meeting. The CMS OBC certification is specific to DHHR's configurations, integrations and any custom development, therefore the environment needed to produce the certification evidence, conduct the independent audits is required to be facsimile of the production environment for go-live. Post go-live, the AuthentiCare CMS certification SME will work with DHHR in preparing the key performance indicator reports required as well as preparation of the demonstration criteria for the final certification review.		
PM091	The Vendor's Operational Readiness Review (ORR) testing should include a volume/stress test of at least 30 calendar days of production-capacity volumes to demonstrate that the solution and Vendor staff members are prepared for full production.	Project Management
AuthentiCare as a SaaS solution has the same code base, architecture, and infrastructure across our customer base. DHHR is looking for a tight timeframe for implementation and doing a specific test setup for volume and stress (performance) testing would add time to the implementation timeline. Our suggestion is to analyze the capacity volumes anticipated by DHHR and provide a performance data report based on currently implemented customers with similar or larger volumes and configurations. This is an alternative to the specific performance testing and based on live production data rather than estimated volumes that may or may not be attained within the first 30 days.		

Req. ID #	Requirement Text	Requirement Type
PM092	The Vendor should document and propose solutions, and timeframes for corrective actions to all issues, problems, and defects identified through the Operational Readiness Review (ORR).	Project Management
The CMS ORR for EVV requires that the vendor provide a Corrective Action Plan for issues identified as part of the CMS formal ORR review. In addition, CMS recommends that the Security and Privacy third-party Audit Security Privacy Assessment Report (SAR) and Penetration testing be complete prior to scheduling the ORR session with CMS. This is to allow for any corrections of critical security and privacy issues to be resolved prior to go live. The AuthentiCare ORR with DHHR would also include review of any open defects, risks and issues and resolution plan for any critical high impact defects correction required for go live.		
PM093	The Vendor should prepare and submit to the Department an Operational Readiness Review (ORR) Report that demonstrates that the Vendor and solution are ready to begin operations.	Project Management
The AuthentiCare delivery team and CMS certification SME would work with DHHR in providing the required evidence documentation for the CMS certification criteria as well as any specific DHHR requirements for ORR in advance of the ORR meeting. The CMS ORR items that will be submitted to the state for review prior to DHHR submission to CMS include: • Test and report with screen shot evidence of the OBC Criteria EVV 1 (21st Century Cures Act data captured), EVV 3 (Visit capture), EVV 4 (data standards), EVV 5 (Avoid paying unauthorized unapproved services), EVV 6 (data flows and interfaces), and EVV 7 (Alternate visit submission modes) • Criteria and evidence will be provided for EVV 2 (data capture if communications are unavailable) • EVV 8 (ADA compliance) an independent 508 test report and EVV (Training and Outreach) the Training plan, training materials and training attendance and outreach documentation Criteria Security 1 requires a third-party Security Privacy Assessment Report (SAR) and Penetration Test and the summary report will be provided to DHHR and to CMS. CMS has requested the independent audit summary report and specifically does not request the full detail report that may expose specifics on a vendor's infrastructure or operations that could compromise security.		
PM094	The Vendor should correct any report errors identified by the Department or the Vendor and correct the report within an agreed upon timeframe, through additional steps as defined in the Change Management Plan, including, but not limited to:	Project Management
PM095	Correct the report	Project Management
PM096	Verify the report	Project Management
PM097	Distribute or re-distribute the report	Project Management
PM098	Others actions as defined by the Department	Project Management
Report errors identified will be corrected pre-production as defined Testing Plan and post production as part of the incident response process. Changes requested will follow the agreed-upon Change Management Plan.		
PM099	The Vendor should assist the Department with specialized research and reporting as requested.	Project Management
FDGS understands that the Department may require special research and reporting to support intelligent decision making and special requests from stakeholders including the Governor's office and the legislature. As we have done for our other AuthentiCare customers, FDGS will work with DHHR on prioritizing change requests based on the agreed-upon Change Management Plan.		
PM100	The Vendor should be able to test edits, business rules, and workflow processing and report on results.	Project Management
FDGS has a dedicated team of testing subject matter experts that comprise our TCoE pool of resources. The TCoE pool of resources is equipped with the processes, technology, tools, infrastructure, and talent to support quality deliverables. The project team will work closely with TCoE pool of resources to provide the highest level of quality assurance throughout the entire lifecycle of the project.		
PM101	The Vendor should support either the transition of the solution to an entity designated by the Department and/or support the retirement of the solution at the end of the term of the contract, including all contract extensions as	Project Management

Req. ID #	Requirement Text	Requirement Type
	defined in the Turnover and Closeout Management Plan.	

FDGS desires to continue to support West Virginia into additional re-procurements. In the event that another vendor is selected to replace the AuthentiCare solution at the end of the current contract, FDGS will provide seamless transition support to maintain exceptional service for providers and recipients up to cutover to the replacement vendor.

In many of our long-term relationships for EVV services, FDGS has been awarded the opportunity to continue services seamlessly into the next contract. As a proprietary SaaS offering, FDGS must protect its intellectual property and we cannot provide our application to the Department as an on-premises or hybrid implementation during the turnover phases at the end of the contract term.

Besides the AuthentiCare application itself, our EVV solution includes a series of shared services that provide a world-class solution for operations and customer support, security and privacy, disaster recovery and business continuity, and product improvements. These shared services must be incorporated into the replacement EVV solution approach either by the Department or a new vendor.

By continuing with the subscribed services that are part of the overall AuthentiCare EVV SaaS offering, DHHR benefits from the functional capabilities of the application and receives continuous improvements and application enhancements that are driven by our interaction with all of our state and federal stakeholders. Without AuthentiCare's continuous improvements and enhancements, the EVV solution becomes stagnant and falls behind our other customers' product and support levels. As usual with any SaaS offering, when the subscription ends, access to the application and related services also comes to an end.

Experience for a Smooth Transition

FDGS understands the need for the Department to bring contracts to a close with its vendors while maintaining all business processes and operations. FDGS has experience with EVV turnovers and completed one EVV turnover in Oklahoma in October 2014. Oklahoma was dissatisfied with the other vendor and returned to FDGS in July 2016, and since then has continued operations with AuthentiCare. We invite the Department to discuss these transitions with our Oklahoma references noted in Proposal Section 2.5 References.

If the Department decides to go to another vendor in the future, FDGS will support the needs of the Department to transfer appropriate data to the Department or to a third-party vendor. FDGS will work to provide a seamless transition. FDGS will commit to complete the initial draft of the Turnover Plan prior to the end of our implementation phase. Once we move into Maintenance & Operations (M&O), FDGS will review and update as required throughout the contract. As we move through the final portion of the contract, FDGS will provide a final plan approximately nine months prior to the end of the contract. Turnover activities will begin according to the plan from approximately nine months prior to the end of the contract until all approved transfer duties are complete within an acceptable turnover timetable.

FDGS recognizes the need to maintain the EVV solution in a full operation mode through the last processing date of the contract. For a successful turnover, we transfer the operational data required for conversion or migration of all work in progress. FDGS will work closely with the Department to identify and provide such information as appropriate and deemed necessary.

PM102	The Vendor should obtain Department approval of all scripts prior to implementation that will be used in the Technical Call Center.	Project Management

Prior to go-live, FDGS will review all scripts prior to use by our Call Center. We will work with DHHR to update and approve those scripts that are specific to DHHR's AuthentiCare jurisdiction.

PM103	The Vendor should identify and be responsible for the implementation and integration of all third-party software used in support of the solution.	Project Management

FDGS incorporates strong code management policies and procedures to validate that no superfluous or unauthorized code is included in the AuthentiCare configuration management suite. The AuthentiCare EVV solution will meet or exceed DHHR system security practices, configurations, and procedures preventing the inclusion of any code of unknown origin.

PM104	The Vendor should conduct requirements validation and joint application design in support of requirements analysis and solution design activities as agreed upon by the Department.	Project Management

Planning The FDGS Team confirms that the project's strategic goals are met by verifying that project management disciplines are planned and performed according to best practices and defined in the Project Management Plan (PMP).

FDGS will facilitate a joint review of RFP requirements with DHHR and designated business and policy stakeholders,

Req. ID #	Requirement Text	Requirement Type
resulting in an approved baseline EVV Solution Requirements Traceability Matrix (RTM). During the joint review of the requirements, FDGS will demo the EVV solution to show how it satisfies the requirements, identify configurable features and functions, and identify any gaps in the EVV solution. Using the RTM, we hold iterative AuthentiCare Design Sessions and validation sessions to clarify and detail the components of the current System Integration Plan (SIP) and business rules of the DHHR AuthentiCare solution to meet the approved requirements. Using the RTM, we hold AuthentiCare Design Sessions to detail the components of the current SIP and business rules of the DHHR AuthentiCare solution to meet the approved requirements. The FDGS Team will update the DHHR AuthentiCare System Documentation based on the Design Sessions and the required business rules. Following the Design Sessions, we will update the RTM, SIP, and AuthentiCare System Documentation based on specific requirements, and provide these items to DHHR for review and acceptance. This EVV configuration and detailed system design documentation is comprised of: • System Integration Plan (SIP) • Appendix B (Imports/Exports) • Appendix C (IVR Script) • Appendix D (Language Packet) • Appendix S (Web Services), if necessary The SIP and AuthentiCare Detailed System Documentation must be approved by DHHR prior to the initiation of the Configuration and Development phase.		
PM105	The Vendor should maintain a requirements traceability matrix (RTM) throughout the lifecycle of the project.	Project Management
The RTM is tracked and maintained as defined in PM104.		
PM106	The Vendor should provide all stakeholders identified by the Department access to the requirements traceability matrix (RTM).	Project Management
The RTM is tracked and maintained as defined in PM104 as well as having changes approved and accepted by DHHR.		
PM107	The Vendor should document in the requirements traceability matrix (RTM) where each requirement is accounted for, including, but not limited to:	Project Management
PM108	Design documentation	Project Management
PM109	Code modules	Project Management
PM110	Test conditions	Project Management
PM111	Test scenarios	Project Management
PM112	Test cases	Project Management
PM113	Certification criteria	Project Management
PM114	Medicaid Information Technology Architecture (MITA) business areas and processes	Project Management
PM115	Medicaid Information Technology Architecture (MITA) Standards and Conditions	Project Management
PM116	Others as defined by the Department	Project Management
AuthentiCare documents RTM traceability for each requirement, functionality, and test condition throughout QA and UAT. Testing vendor staff and assigned DHHR staff will have access to the CAT environment to execute UAT. FDGS will work with the Department to develop detailed test scenarios to support UAT. These detailed test scenarios will allow DHHR to test all functional aspects of the system and confirm performance in accordance with the specifications and the approved RTM. Our project and technical teams will provide support throughout this process, which includes answering questions, researching issues, executing corrections, and retesting software components. These capabilities provide DHHR with the confidence that its EVV project adheres to sound project management and		

Req. ID #	Requirement Text	Requirement Type
development standards within the Health and Human Services industry, and that the EVV Project meets federal requirements for certification and enhanced federal funding. As an integral partner with DHHR, as well as its regional CMS representatives, AuthentiCare provides an experienced, insider perspective on satisfying CMS mandates and state imperatives. The combination of the AuthentiCare solution, FDGS' proven MITA compliance, and CMS certification experience is unmatched in the current marketplace.		
PM117	The Vendor should demonstrate through the requirements traceability matrix (RTM) that all documented and approved specifications have been traced throughout the development lifecycle.	Project Management
AuthentiCare will provide the RTM for review for each requirement, functionality and test condition throughout QA and UAT. Testing vendor staff and assigned DHHR staff will have access to the CAT environment to execute UAT. FDGS will work with the Department to develop detailed test scenarios to support UAT.		
PM118	The Vendor should work with the Department during joint application design (JAD) sessions to validate the scope, purpose, and implications of each Request for Proposal (RFP) specification.	Project Management
Using the RTM, we hold iterative AuthentiCare Design Sessions and validation sessions to clarify and detail the components of the current System Integration Plan (SIP) and business rules of the DHHR AuthentiCare solution to meet the approved requirements. Using the RTM, we hold Design Sessions to detail the components of the current SIP and business rules of the West Virginia AuthentiCare solution to meet the approved requirements. The FDGS Team will update the DHHR AuthentiCare System Documentation based on the Design Sessions and the required business rules. Following the Design Sessions, we will update the RTM, SIP, and AuthentiCare System Documentation based on specific requirements, and provide these items to DHHR for review and acceptance.		
PM119	The Vendor should identify and work to resolve gaps between the Vendor's and the Department's understanding of a specification(s) during joint application design (JAD) sessions.	Project Management
Design Session deliverables will be provided for DHHR gap review subsequent to the process defined in PM118.		

8.2 Implementation Methodology

RFP Section Attachment 9 – 3-3.6.5.5.2.3, pp.124-131

3.1 The Vendor should respond to the headings below and describe the overall approach for the following areas of system development life cycle (SDLC) and support.
3.2 The Vendor's proposal should include in its response what the Vendor believes will be an effective process for each component and flow between each of the following areas:
3.2.1 Requirements Analysis and Solution Design Methodology
3.2.2 Solution Development
3.2.3 Data Conversion
3.2.4 Testing

3.3 Requirements Analysis and Solution Design Methodology
3.3.1 The Vendor's proposal should describe the Vendor's approach to requirements analysis and the design of the solution. This should include in the response a description of what the Vendor believes will be an effective System Architecture and Design methodology.
3.3.2 During the solution's design, the Vendor should conduct requirements analysis, during which it reviews, refines, and seeks approval for all preliminary requirements included in this RFP, and add requirements where gaps are identified through a detailed analysis exercise. The result should be a final set of detailed requirements to be used for configuring and building the Electronic Visit Verification (EVV) solution. These requirements should be the basis for the Vendor to create usage scenarios and detailed business process workflows.
3.3.3 During the solution's design, the Vendor should develop detailed specifications that demonstrate that the solution meets the information technology (IT) needs to support business processes. The system requirements and logical description of the entities, relationships, and attributes of the data that were documented during the requirements analysis should be further refined and allocated into system and database design specifications that are organized for implementation within the constraints of a physical environment.
3.3.4 The Vendor and DHHR should conduct a formal review of the high-level architectural design prior to detailed design of the automated system/application to achieve confidence that the design satisfies the system requirements and is in conformance with the enterprise architecture and prescribed design standards.
3.3.5 The solution design and its multiple components should be developed in conjunction with the Project Work Plan as follows:
3.3.5.1 The first component should be a Preliminary System Design, which outlines the overall functions that will be developed, their interactions, components, and high-level architecture.
3.3.5.2 The second component should be a Detailed System Design (DSD), which will give the planned implementation details of the design for each component, interactions, and place in the overall technical architecture.
3.3.5.3 The third component should be the Final System Design, which will give the actual implementation details of each component and sub-component from a functional and technical perspective, including the final architecture implementation.
3.3.6 The Vendor's proposal should also describe its approach to conducting requirements validation sessions and Joint Application Development (JAD) sessions. The Vendor's proposal should also include the number and topics of the sessions to be held in support of both requirements validation sessions and JAD sessions.
3.3.7 The Vendor's proposed approach to requirements analysis and solution design should also include detail on the following:
3.3.7.1 Process for identifying and resolving gaps between the Vendor's and DHHR's understanding of an RFP specification.
3.3.7.2 How the solution's design will include collaborative design with functional and technical subject matter experts.
3.3.7.3 How the Vendor intends to obtain DHHR approval on RFP specifications.
3.3.7.4 Description of how the proposed solution will fulfill the Medicaid Information Technology Architecture (MITA) requirements.
3.3.7.5 Design documentation for all those project deliverables delivered during the Solution Planning and Solution Design, Testing, and Operational Readiness task groups.
3.3.8 The Vendor should propose an approach describing how the EVV design will integrate with other EVV components and DHHR enterprise. The Vendor should also propose how design decisions will be coordinated across all functional areas and modules.

3.4 Solution Development Methodology
3.4.1 During the Development Phase, the Vendor's system development team should take the detailed logical information documented in the System Design Phase and transform it into an executable form to ensure that all individual components of the automated system/application function correctly and interface properly with other

components.
3.4.2 The Vendor's proposal should describe the Vendor's System Development methodology. Include in the response a description of what the Vendor believes will be an effective system development methodology (e.g., Waterfall, Rapid Application Development) for both the Vendor and for DHHR during the implementation of the proposed solution.
3.4.3 The Vendor's proposal should present a narrative description of the Vendor's proposed approach to solution development, including the Vendor's proposed:
3.4.3.1 Software/hardware solution, including a description of the solution's ability to accommodate the current and future business and technical needs of DHHR's Medicaid Enterprise. The solution should also describe the methodology and approach for the following:
3.4.3.1.1 Regular system maintenance, performance optimization, resource capacity utilization, capacity planning, and capacity expansion.
3.4.3.1.2 Compatibility of all hardware, software, or communications components installed for use by DHHR staff with the most current West Virginia Office of Technology (WVOT)-supported versions.
3.4.3.1.3 Methodology and approach for implementing and maintaining solution documentation, including data structures, Entity Relationship Diagrams (ERDs), user manuals, Business Rules Engine (BRE), and all other documentation related to the EVV platform, operating system, and programming language.
3.4.3.1.4 Methodology and approach to preparing, maintaining, and distributing user documentation for each business process, including a description of how it is to be used as the basis for User Acceptance Testing (UAT) and training, as well as the use of final versions for training before the start of operations.
3.4.3.1.5 Methodology and approach to programming and unit testing on all system functions to ensure that a single component can function correctly on a standalone basis.
3.4.3.1.6 Methodology and approach to ensure that the developed solution meets design criteria.
3.4.3.1.7 Methodology and approach to ensure installation and enhancement or modification of the components of the proposed solution meets the specifications developed and approved by DHHR.

The Department benefits with AuthentiCare as its EVV solution by building on years of maturity and implementation of the solution across seven other statewide programs and multiple MCOs. We have continued to improve the AuthentiCare software capabilities both functionally and for those non-functional needs including scalability, flexibility, configurability, and definitely, security and privacy.

Besides the software and technical platform of AuthentiCare, our delivery team has matured and enhanced our approach to implementation. We are able to plan and execute more iterative cycles to continuously deploy more and more requirements of each specific agency as we get closer and closer to Go Live and the cutover to production. We plan to use this same implementation approach for the six-month implementation period required for this RFP. With this approach, DHHR will be successful in complying with the 21st Century Cures Act and be ready to complete the activities necessary for CMS certification.

Requirements Analysis and Solution Design Methodology

AuthentiCare is built on a modern, industry standard-based platform. The modular, flexible approach to systems development, including the use of open interfaces and exposed application programming interfaces (APIs) separates business rules from core programming. The FDGS team will work with DHHR to validate requirements and continue through design activities with iterative configuration tasks to tailor AuthentiCare for the DHHR-specific program policies. The flexibility of our configurable solution limits the need for most custom development.

We do not start from a blank slate with the Requirements Traceability Matrix (RTM) for EVV projects. We have built a complete RTM that incorporates the best new features from each project as AuthentiCare is improved. AuthentiCare already includes the functionality for the Cures Act. We will identify those specific requirements from this RFP that need to be added so that they are validated and included in the AuthentiCare Design Sessions.

Using the RTM, we hold iterative AuthentiCare Design Sessions and validation sessions to clarify, refine, and detail the components of the current System Integration Plan (SIP) and business rules as well as identify any gaps of the West Virginia AuthentiCare solution to meet the approved requirements. The FDGS Team will update the DHHR AuthentiCare System Documentation based on the Design Sessions and the required business rules and submit for DHHR approval. Following the Design Sessions, we will update the RTM, SIP, and AuthentiCare System Documentation based on specific requirements, and provide these items to DHHR for review and acceptance.

This EVV configuration and detailed system design documentation is comprised of:

- System Integration Plan (SIP)
- Appendix B (Imports/Exports)
- Appendix C (IVR Script)
- Appendix D (Language Packet)
- Appendix S (Web Services), if necessary

The SIP and AuthentiCare Detailed System Documentation must be approved by DHHR prior to the initiation of the Configuration and Development phase and must reflect how the solution meeting the IT needs to support the DHHR business processes. The system requirements, relationships, and attributes are integrated into the database and system design specifications which are then organized logically for system implementation and integration.

AuthentiCare's integration capabilities are based entirely on open-systems standards and accommodate communications to database management systems and back-end solutions through APIs and custom imports and exports. Additional features, such as Microsoft's BizTalk EDI 837 file creation, are built into the AuthentiCare solution and leverage the open standard architecture.

FDGS makes business rules available in formats that both humans and machines can read. Most business rules in AuthentiCare are captured in metadata tables in the database so that they are easily changed and updated as business rules change. The core programs in AuthentiCare use business rules that are dynamically data-driven by values in metadata tables. This separates the core functions from a specific client's setup and business rules. This meets the modularity standards requirement to separate APIs, business rules, and core code into modules.

FDGS uses the MITA conditions and standards for the development and deployment of the AuthentiCare EVV solution. We have a strong understanding of MITA and its emerging industry changes. Our knowledge of MITA and MMIS systems will benefit to DHHR in potential projects involving health care information technology and the migration to a modernized platform.

FDGS' AuthentiCare solution architecture and design applies industry standards whenever applicable industry standards exist. This makes the solution highly modular, extensible, interoperable, and flexible. FDGS understands the necessity of protecting the privacy and confidentiality of your data. The AuthentiCare solution provides world-class security thanks to FDGS' global security practices and procedures. The EVV system meets the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA compliant practices include:

- Data transfers employ AES 256-bit encryption and TLS 1.2 or SFTP
- Users are individually registered and functional rights and roles are assigned to their login credentials
- Both IVR and Mobile App employ two-factor authentications as required
- Users are data scoped to see only relevant data that they are allowed to see
- ANSI X-12 transactions are employed where relevant

With regard to accessibility standards, FDGS has engaged Level Access to advise us as to accessibility and use with assistive technology for the AuthentiCare Web and Mobile App. Level Access has provided third-party ADA Section 508 certification of both the Web and Mobile applications. Additionally, due to the integration into the Texas Medicaid space, the system, including mobile and TTY meet WCAG 2.1 accessibility standards.

The AuthentiCare solution is inherently a Software-as-a-Service (SaaS) solution and the interfaces to use it are sharable and reusable within West Virginia agencies. In particular, the Mobile App supports multiple configurations with different business rules. The business rules set is selected by a configuration code, while user preferences are applied when the user logs in. This is achieved with only one common app each in the Apple App Store and Google Play. The AuthentiCare solution is in full production in several states, with each state having the solution modules relevant to their specific business and program needs. Additionally, modules can be deferred for integration based on schedule and level of complexity of enhancements.

3.5 Data Conversion Strategy, Approach, and Timeline
3.5.1 The Vendor's proposal should describe what the Vendor believes to be an effective data conversion strategy and approach for supporting migration of data from the current solution (Section 4.1: Background and Current Operating Environment) to the proposed solution (Section 4.2: Overview of Expected Medicaid EVV and Supporting Services).
3.5.2 The Vendor's proposal should also describe how the Vendor will ensure data integrity and consistency through all phases of the project.

Data Conversion

The FDGS Master Test Plan (MTP) for AuthentiCare EVV solutions provides a full lifecycle approach to all required testing sub-phases. While AuthentiCare is offered as a SaaS solution, it is a framework that we configure specifically for the DHHR EVV business processes. Our teams provide system testing through our Quality Management and Testing approach as well as User Acceptance Testing (UAT) support to the Department. Data conversion is crucial functionality and will be a priority in all phases of the project to confirm that the data exchanged in the DHHR solution meets all requirements and enables all business units effected, as well as the MMIS to function appropriately. Data interchanges will be identified in the planning phase and during the development phase, all integration specifications will be designed and accepted by DHHR. Data integration must occur using file exchange through approved File Gateway methods to keep PII/PHI secure.

3.6 Testing
The primary purpose of the Testing Phase is to determine whether the developed solution is ready for implementation. During the Testing Phase, formally controlled and focused testing is performed to detect errors, issues, and defects that need to be resolved.
DHHR envisions the stages of the Testing Phase occurring concurrently with the Development Phase, with testing for each development iteration.
3.6.1 Testing should occur throughout the development process, and the initial planning for testing activities should occur early in the project. DHHR recommends that planning for the Testing Phase occur as early in the

project as possible to ensure successful testing results.
3.6.2 The DHHR defines the types of testing as follows:
3.6.2.1 Unit Testing: Unit testing assesses and corrects the functionality of individual or small groups of code or modules. Unit testing ensures the various objects and components that make up the system are individually tested, and that errors are detected and corrected prior to exiting the development environment.
3.6.2.2 Integration Testing: Developers perform integration testing after integrating completed components or modules into the overall system codebase. This testing ensures that the completed components or modules work at a level of efficiency acceptable by DHHR and that existing components and shared components have not been broken by the new module.
3.6.2.3 Iterative Functional Testing: Iterative functional testing ensures that the components developed for each logical iteration of the system meet all functional and technical requirements as defined and approved by DHHR.
3.6.2.4 System Integration Testing: System testing assesses the functionality and interoperability of the solution and the multiple other systems and subsystems it interacts with, such as databases, hardware, software, rules engine, document management system, identity management system, workflow, interfaces, and web services, and their integration with infrastructure into an overall integrated solution. This test includes a test installation and configuration of the solution, with a subsequent functional regression test to confirm the installation's success.
3.6.2.5 Interface Testing: Interface testing ensures the completeness of interface development and the readiness of developed interfaces for integration in the wider system.
3.6.2.6 Regression Testing: Regression testing assesses the integrity of the solution subsequent to the deployment of new solution components and/or fixes.
3.6.2.7 End-to-End Testing: End-to-end testing is a quality assurance testing methodology that strives to ensure correct functioning and performance of applications in production-like scenarios. This methodology checks if an application performs as designed on all levels and across all subsystems. It is intended to encompass testing for solution's key business and functional processes in their entirety from their start through completion.
3.6.2.8 Security Testing: Security testing is the testing of functional, technical, infrastructure, and operational solution components to ensure the solution and operations meet all security requirements.
3.6.2.9 Performance Testing: Performance testing ensures that the solution meets the minimum performance service levels required by DHHR, in terms of query and page response times under simulated load for a number of users for multiple concurrent functions in a given period. Performance testing scenarios take into account expected peak period volumes for application processing such as closing of open enrollment periods.
3.6.2.10 Usability/Accessibility Testing: Usability testing ensures the solution user interface design takes into account usability considerations for its target user groups.
3.6.2.11 Browser Testing: Browser testing ensures that the solution operates in the most likely configurations of browser versions and operating solutions. The Vendor is responsible for providing the machine configurations to perform all necessary browser testing. Browser testing also includes the testing of mobile view and mobile browsers.
3.6.2.12 User Acceptance Testing (UAT): UAT ensures that the developed system meets all expectations of DHHR and all solution users. UAT test scripts cover all facets of the system, and the Vendor should be responsible for drafting all UAT scenarios and cases per DHHR's direction. DHHR will be responsible for identifying the participants involved in UAT, for the overall execution of UAT scripts, and for any ad-hoc UAT testing.
3.6.2.13 Data Conversion Testing: Data conversion testing ensures that data migrated from the current solution are brought across to the new solution in a usable, complete, correct, and expected state
3.6.2.14 Operational Readiness Testing (ORT): ORT is performed to examine the operational capability of the solution and its associated processes and procedures. ORT focuses on the validation or verification of the processes involved primarily outside of the system.
3.6.2.15 Parallel Testing: Parallel testing is a method of comparing the activities and/or data of the old solution against the new solution. In order to reduce risk, the old and new solutions run simultaneously for some period of time after which, if criteria for the new solution is met, the old solution is disabled.
3.6.3 The Vendor's proposal should describe the Vendor's understanding of the aforementioned testing types, and should include detail on the approach and methodology for the following:
3.6.3.1 All aforementioned testing types, as well as any others the Vendor plans to deploy
3.6.3.2 Timing for execution of each testing type
3.6.3.3 Usage of tools the Vendor proposes be used in support of each testing type
3.6.3.4 Testing environments to be used in support of each testing type, and for all necessary testing activities
3.6.3.5 Validating the traceability of requirements throughout the full testing process
3.6.4 The Vendor's proposal should also include detail on the Vendor's proposed source code management tool, as well as details on the project repository that will be used to store usage scenarios, use cases, requirements, designs, test scenarios, test cases, test results, and other project artifacts.
3.6.5 The Vendor's proposal should also present a narrative description that includes the following:
3.6.5.1 Approach to completion of the Solution Design, Testing, and Operational Readiness task group's testing-

related deliverables.
3.6.5.2 Approach to obtaining DHHR's approval of the testing-related project milestones including the proposed acceptance criteria for each milestone.
3.6.5.3 Approach to:
3.6.5.3.1 Working with federal partners, DHHR, the Project Management vendor, the Independent Verification and Validation (IV&V) vendor, and/or any other vendor throughout all testing phases
3.6.5.3.2 Developing test cases and scripts to thoroughly test system functionality
3.6.5.3.3 Supplying documentation of each testing type
3.6.5.3.4 Preparing data for each testing type
3.6.5.4 Details on the support the Vendor intends to supply during UAT, such as the Vendor's approach to:
3.6.5.4.1 Developing the UAT Plan, scripts, cases, timeline, and supporting processes
3.6.5.4.2 Preparing test data
3.6.5.4.3 DAT results analysis, identification of defect severity, and defect resolution
3.6.5.4.4 Defect tracking, repair, and reporting
3.6.5.4.5 UAT final report that includes:
3.6.5.4.5.1 A written certification letter certifying that UAT was successfully completed
3.6.5.4.5.2 A list of all defects and issues
3.6.5.4.5.3 A list of all resolved critical defects and/or issues
3.6.5.5 The Vendor's proposal should also include detail on the approach to ORT including details on:
3.6.5.5.1 ORT approach
3.6.5.5.2 ORT final report that includes:
3.6.5.5.2.1 1 A written certification letter certifying that DAT was successfully completed
3.6.5.5.2 2 A list of all defects and issues
3.6.5.5.2.3 A list of all resolved critical defects and/or issues

Testing

FDGS follows a disciplined Quality Assurance (QA) approach that contributes to our record of delivering projects on time, within budget, and with high quality. This Structured Test Methodology (STM) verifies that all functional and system-wide requirements are complete and confirms the configuration requirements.

Our team uses quality assurance management processes and controls, which are documented in the overall TCoE testing process. The testing approach, objectives, schedule, and procedures are documented in our test plan along with phase entrance and exit criteria. Entrance criteria is documented along with the primary responsibility for each item. Entrance criteria includes:

- Requirements completed, reviewed, and signed off (AuthentiCare Product Team)
- Design completed with stakeholders' sign-off (AuthentiCare Design Team)

FDGS performs extensive testing for all implementations and configurations per our Software Development Life Cycle. From the iterative requirements gathering sessions, the unique requirements of DHHR are identified and the specific system configuration items documented. Our technical teams implement the required configuration into our Quality Assurance (QA) test environment. Our TCoE pool of resources develops a Master Test Plan based on the system configuration identified. The Master Test Plan includes activities to cover unit, system integration, interface, performance/stress, and browser-based testing.

FDGS uses its production-comparable Quality Assurance (QA) environment to complete performance and load testing activities. The technical team uses IBM Rational Performance Tester to identify system performance bottlenecks, reduce load testing, and analyze the impact of load from the different AuthentiCare application components.

Our QA Team designs, builds, and executes test scripts so that application features are confirmed throughout configuration management activities. Testing results conducted by the FDGS testing team will be documented and summarized for DHHR to review as part of the

System Integration Testing deliverable. FDGS will submit SIT test results to DHHR for approval prior to the migration to UAT.

Test cases are documented as are the results. The testing activity including the Master Test Plan can be shared with DHHR if requested. Using mock data for our QA and UAT testing (avoiding any PHI or PII concerns), test data are created by the TCoE pool of resources as well as test scenarios.

When the requirements of the Master Test plan are complete in QA, the implementation is promoted to our User Acceptance Test (UAT) environment. Additional test data are added to this environment, DHHR is invited to perform additional testing, and an Application Security Assessment (ASA) is initiated with FDGS' Global Cyber Security and Fraud group.

FDGS follows a disciplined Quality Assurance (QA) approach that contributes to our record of delivering projects on time, within budget, and with high quality. This Structured Test Methodology (STM) verifies that all functional and system-wide requirements are complete and confirms the configuration requirements. In support of the STM, FDGS has a dedicated team of testing subject matter experts that comprise our TCoE pool of resources. The TCoE pool of resources is equipped with the processes, technology, tools, infrastructure, and talent to support quality deliverables. The project team will work closely with TCoE pool of resources to provide the highest level of quality assurance throughout the entire lifecycle of the project.

FDGS' Unified Vulnerability Management Services (UVMS) Team's primary responsibility is to perform periodic penetration tests and vulnerability assessments of FDGS' infrastructure and applications. UVMS plays a vital role in helping to protect customer information and the assets of FDGS. UVMS employs a variety of technologies, tools, and techniques to help make sure that high-quality security assessments are performed. Security assessments identify vulnerabilities that may represent varying degrees of risks to FDGS. Vulnerabilities deemed of risk to FDGS are assigned to appropriate individuals who are required to take action to mitigate any risks associated with identified vulnerabilities.

Penetration Testing: Penetration testing is conducted to comply with FDGS policy, customer mandates, and Payment Card Industry Data Security Standard (PCI-DSS) requirements. The purpose of penetration testing is to measure the security posture of a target system or environment. Penetration testing is not simple hacking but, instead, is a process designed to validate security weaknesses, identify attack vectors, and validate the functionality of security controls. The penetration testing process FDGS uses is a 'gray' box approach as defined in NIST 800- 115 Technical Guide to Information Security Testing and Assessment. Penetration tests are designed to be nondestructive, and minimize the potential impact to systems or networks under test.

Third-Party Penetration Testing: UVMS facilitates an annual third-party security assessment of external networks. These tests are performed in addition to UVMS testing, and are executed by an approved, independent third party. Only GCSF-approved vendors are authorized to execute testing on FDGS' behalf, in accordance with FDGS policy.

Vulnerability Scans: A vulnerability scan is an automated process that is designed to assess computers, computer systems, networks, or applications for security vulnerabilities or weaknesses. While functionality varies between different types of vulnerability scanners, they share a common, core purpose of enumerating the vulnerabilities present in one or more targets. In accordance with FDGS policy, UVMS uses Nessus and Trustkeeper to perform regular vulnerability scans of FDGS' network and computer systems. The scanning tools used

are considered industry standard and are customized to test FDGS networks in an efficient manner, while minimizing the potential risks associated with active scanning. Vulnerabilities deemed of risk to FDGS are assigned to appropriate individuals who are required to take action to mitigate any risks associated with identified vulnerabilities.

Testing Results: FDGS UVMS tracks and reports on results of the security assessments performed. Results of ad hoc assessments performed outside of normal testing cycles are provided to the requester, system owner, and the Cyber Risk Manager responsible for the network or system under test.

People: UVMS personnel are required to meet minimum qualification standards. Industry and military experience, educational background, and certifications are the basis for making hiring decisions.

Governance: The operations of UVMS are governed by FDGS' Global Cyber Security Policy and Standards. UVMS objectives encompass areas such as the frequency of vulnerability tests, the scope of the assessment, and the required outputs of the process. Objectives are reviewed annually, or as necessary when policy changes are made, to validate consistency with the Global Cyber Security Policy.

Methodologies: UVMS has formal, documented assessment methodologies and procedures in place describing the processes and steps to be followed when performing security assessments. These documents give general information regarding the process to initiate, approve, perform, and conclude security assessments, as well as procedures for using each of the security assessment tools.

Logical and Physical Access: Because of the sensitive nature of the tools used and procedures performed by UVMS, specific security measures have been taken to restrict access to UVMS systems. Logical access to the systems from which vulnerability assessments are performed is restricted to UVMS staff. UVMS staff must individually authenticate to each server with a public/private key pair in order to access the security assessment tools.

Physical access to UVMS systems and facilities is restricted to authorized individuals only. Access to the Cyber Vulnerability Center is maintained, administered, and controlled by Corporate Security. Additionally, an electronic record is maintained by Corporate Security of access to secured areas.

8.3 Deployment Methodology

RFP Section Attachment 9 – 4, pp. 131-133
4.1 Describe the Vendor's overall approach regarding the following areas of SDLC and support. The Vendor's proposal should include in its response what the Vendor believes will be an effective process for each component and flow between each of the following areas:
4.1.1 Implementation/Rollout Planning
4.1.2 Implementation Methodology and Timeline
4.1.3 Issues, Challenges, and Risks
4.1.4 Lessons Learned

AuthentiCare's Implementation Planning

Deployment begins in synchronization with the configuration phase. This approach allows for a base product environment to be implemented early in the process and base functionality can be demonstrated and discussed prior to making costly customizations. Additionally, the Client Acceptance Testing environment for User Acceptance Testing is made available to provide a more collaborative experience for DHHR staff with AuthentiCare. Data imports are also tested and approved in this phase.

While it is called the "deployment" phase, this is also the majority of the training planning, materials, and production phase. All training materials will be planned in tandem with DHHR and then materials will be produced and collaboratively edited to produce the highest quality of items to meet approved requirements. Marketing outreach is essential for providers to understand and prepare for the transition, and is done in harmony with the training materials so that look and feel is consistent for all user groups.

Built on a Service Oriented Architecture (SOA), our hosted solution is deployed after business hours and promoted to a production environment after User Acceptance Testing but before the go-live date. Data centers are tested for redundancy in the production environment to provide for business continuity. During deployment, if issues or risks are identified, they will be logged into the risk management or issue management logs and mitigated or assumed in accordance with the decisions of DHHR. Lessons learned sessions will be conducted approximately 30 days post go-live with DHHR stakeholders and FDGS key personnel.

Implementation Methodology and Timeline

In this section, we provide a description of our SDLC methodology and approach based on multiple statewide implementations of AuthentiCare and with MCOs. FDGS repeats its EVV implementation phased approach using its Baseline Project Plan broken down into six major phases: Initiation, Planning, Configuration, Deployment, Operations (Production Readiness), and Close Out. FDGS addresses DDI through different activities or phases to complete its system development lifecycle (SDLC) and to configure the AuthentiCare product to the specific requirements of this RFP. We begin by combining Design and Development together as we identify the unique requirements of DHHR and move through our design sessions. Product quality is integral to conclude the development portion of our project plan, therefore, we have included our approach and plan for system testing. Finally, we look at the overall implementation methodology phases and preparation for Go-Live.

Issues, Challenges, and Risks

The aggressive timeline for implementation pairs well with the AuthentiCare implementation with configurations. The more state specific customizations requested in the first deployment the

more risk to the timeline and challenges. Creating a backlog of future requirements and design items for after the first deployment is a best practice for proactively mitigating.

Lessons Learned

At the request of DHHR, the implementation period for EVV in West Virginia is six months and that does carry in some risk for on-time deployment because resources from the Department and supporting agencies, such as Information Technology, will have to be available with shortened turn-around times for decisions and approvals. Lessons learned will be key in delivering enhancements during the M&O phase for the project and it will remain a challenge to stay in the deployment windows without having to defer functionality to the M&O phase with enhancements.

8.4 Training

RFP Section Attachment 9 – 5, 4.4.3.2, pp. 133-134, 54

5. Training
5.1 The Vendor's proposal should present a narrative description of the Vendor's proposed approach to completion of the training throughout the contract, including the Vendor's proposed:
5.1.1 Approach to the completion of the training deliverables (as listed in Appendix 2: Deliverables and Milestones Dictionary), including methodology for updating deliverables throughout the lifecycle of the project.
5.1 2 Approach to development, maintenance, and implementation of the Training Management Plan, including methodologies addressing:
5.1.2.1 Assessment of internal and external training needs, including gap analysis
5.1.2.2 Approach to user training, supporting all business processes as identified in the RFP
5.1.2.3 Delivery of end-user training throughout the solution's implementation
5.1.2.4 Development and use of online tutorials, online help, online policy and procedure manuals, and hard copy user manuals for the delivery of training
5.1.2.5 Development and use of live, web seminar, and video-based training
5.1.2.6 The target audiences for training, including DHHR staff, Vendor staff, clients, providers, and third-party stakeholders that work in the system
5.1.2.7 Plan to provide and/or leverage existing DHHR training facilities to perform end-user training detailed in this section
5.1.2.8 Tools that the Vendor will use to support training
5.1.2.9 The planned curriculum for each system user role and audience
5.1.2.10 Initial training schedule
5.1.2.11 Version control and maintenance of training documentation
5.1.2.12 Training evaluation, including the use of evaluation survey tools to determine whether the trainings produced the expected results
5.1.2.13 Initial and ongoing training outcomes tracking and reporting, including information such as, but not limited to, the number of training sessions, type of training, training locations, number of trainees, and information regarding the actual training results and recommendations for follow-up training
5.1 2.14 Approach to "train-the-trainer" activities during the Operations phase
5.1.3 Approach to role-based training during both implementation, and maintenance and operations
5.1.4 Approach to development of training materials
5.1.5 Approach to training evaluations

This sub-section describes our approach to Training.

FDGS will provide training for DHHR staff, providers, and other users, beginning in the Deployment Phase according to the agreed-upon Training and Outreach Plan. Training users prior to implementing a production environment is critical to successfully onboarding providers. In previous implementations, multiple sessions were held in a variety of locations allowing providers an opportunity to receive training and use the testing environment without impacting records in the production environment. FDGS offers multiple Training and Outreach options to meet the EVV training requirements.

Our Approach

Experience has taught us that training is fundamental to the successful implementation of AuthentiCare and a positive user experience. Our flexible, customized, and comprehensive training methodologies provide ongoing training and education and reflect the voice of the client throughout the life of the contract. We record comments and questions during the training sessions, which provide input for creating future workshops or training opportunities.

We are constantly improving and investing in our training program based on feedback received from system users along with evaluations of the AuthentiCare trainers and training curriculum during the on-site provider sessions.

The new CMS EVV Outcomes Based Certification (OBC) requires, under Criteria EVV9, evidence of the training plan, materials, and a record of scheduled training sessions as well as which groups attended those training sessions. FDGS complies with the requirements of OBC EVV9. We can provide evidence to show that effective outreach and training was provided to assist in onboarding providers and workers, which will support the State of West Virginia in its certification process.

Audience

FDGS understands that transferring knowledge to DHHR staff is a key component to building the skills needed to achieve long-term sustainability of the AuthentiCare EVV solution. The ability to successfully develop the skills of the AuthentiCare user base begins with a clear understanding of the related skills. Knowing this, FDGS will participate in:

- Stakeholder meetings, including on-site meetings as needed
- Web-based outreach and training materials for system users, including providers, support coordinators, and others as deemed necessary by DHHR

Our team will customize materials to meet EVV requirements and will distribute them via email or post them in a secure location for stakeholder access. Online, web-based training will be available post-implementation for users to refresh their knowledge and skills.

FDGS will be available to answer the West Virginia user community's questions, provide guidance, and refresh training concepts via email, telephone, scheduled webinars, and provider update forums.

Training Options

FDGS offers options for training including on-site, instructor-led training, as well as webinars and regularly scheduled provider update forums/assistance calls. The AuthentiCare User Manual will be available to all stakeholders before and after the AuthentiCare solution's implementation.

- **On-site instructor-led training:** FDGS uses quality training materials and experienced trainers who know the AuthentiCare solution. We employ a Train-the-Trainer model, which designates an AuthentiCare expert or trainer within the provider organization, reducing the impact of having all staff unavailable during training at the same time. On-site training allows for the development of in-person relationships with providers and offers opportunities to ask face-to-face questions. Training resources take advantage of user documentation and hands-on application examples to explain AuthentiCare's processing components.
- **Webinars:** Subsequent webinars for process reinforcement and for AuthentiCare enhancements offer providers convenience by using a conference call and online format. The advantage for trainees is the ability to use their own computer, as well as the opportunity to ask questions in real time. FDGS distributes quality training materials and employs experienced trainers who are knowledgeable in AuthentiCare.
- **EVV solution training environment:** A live AuthentiCare training environment available via web and Mobile Applications mirrors real-life test scenarios and daily workflow processes. The advantage for current or new users is the ability to acclimate to the AuthentiCare system in an environment that is isolated from production. The training version of AuthentiCare is always available and is updated at the same time upgrades and product

releases are applied to the production version so that the two environments remain synchronized.

- **Provider forums/assistance calls:** The Account Manager, or designated Subject Matter Expert, leads the forums in person or online. Forums allow training of enhancements and offer the provider community an opportunity to brainstorm among themselves any suggestions they might have to expand AuthentiCare solution's capabilities. These meetings are scheduled on a regular basis to meet provider needs while the EVV solution is in place. Once implementation is complete, monthly provider support calls via conference call or webinar can provide ongoing opportunities for questions, continuing education, and identification of areas where clarification may be needed.



- **Online web-based training:** AuthentiCare includes self-paced, web-based training modules available for providers to review different scenarios on demand. These modules can serve as initial online training or as follow-up training to refresh knowledge and skills. AuthentiCare users may start with any module and move from one module to another at their own pace. The table of contents in each module is designed for forward and backward movement from one topic to another to meet user education needs. The AuthentiCare eLearning environment reinforces the information found in the AuthentiCare User Manual and is part of our collection of training materials.
- **AuthentiCare User Manual:** The training materials in the AuthentiCare User Manual will be tailored to West Virginia's EVV programs. This is a comprehensive user manual that documents and explains system functionality. The advantage is a regularly updated organic document, accessible and searchable online, that reflects changes and enhancements to AuthentiCare functionality. The AuthentiCare User Manual will be updated to reflect enhancements and other system changes identified during design sessions as well as future changes.

Stakeholder Meetings

DHHR staff, provider agencies, and direct care workers will be adjusting to changes and will likely generate a high volume of questions when AuthentiCare is first deployed. FDGS develops a staffing plan that recognizes this increased demand for support and will staff its team accordingly so that all business needs are met.

FDGS has experienced EVV trainers ready to provide additional training opportunities to further the knowledge of EVV to all stakeholders. The following methods provide for continued collaboration and communication with the stakeholder community:

- **Account Management:** An Account Manager will be assigned to DHHR to assist the client with support, training, or communication needs. The Account Manager will coordinate with DHHR on any outstanding needs after the solution is in production.

- **Provider Forum Calls:** The Account Manager and Training Lead will take the lead in hosting post-implementation provider forum calls. Initially, provider forum calls will occur at least weekly for typically one to three months or until experience and comfort is established among the provider community, tapering to a monthly schedule thereafter. The provider forum offers an opportunity for ad hoc training sessions where attendees ask questions and receive answers to issues they are currently experiencing. Furthermore, provider forums enable stakeholders to discuss potential enhancements to AuthentiCare which could better support the provider community's business goals.
- **New Providers:** For newly boarded providers that did not participate in the initial on-site train-the-trainer training sessions, there will be an opportunity to access the AuthentiCare User Manual and other supplemental training aids. If small group training is needed, FDGS will provide one-on-one training to providers to assist them in their transition into AuthentiCare.
- **Release Notes:** When functionality updates are released to the production environment, providers and DHHR staff will be provided release notes documenting the change(s), type of change(s) (enhancement, bug fix), and the impact. When appropriate, FDGS may provide web-based training to walkthrough the release changes.

FDGS provides additional detail to the Training Subject Matter Area requirements in Table 8.3.

Table 8.3 – Detailed Response to Training Requirements

Req. ID #	Requirement Text	Requirement Type
TN001	The Vendor should provide outreach to users to ensure and document their readiness to begin using the solution. The outreach should include all user groups including, but not limited to:	Training
TN002	Members or Legal Representative	Training
TN003	Direct Care Workers	Training
TN004	Provider Agencies	Training
TN005	The Department	Training
TN006	Other as defined by the Department	Training
Our Training Lead will draft a tailored AuthentiCare Training and Outreach Plan shortly following project kickoff. A final version specific for West Virginia's AuthentiCare Training Plan will be submitted for review and approval by DHHR before distribution. The approved Training and Outreach Plan will drive the execution of training and outreach activities for the new EVV solution. FDGS provides thorough training and outreach as part of the overall Training and Outreach Plan. We offer multiple training and outreach options. The Training Lead will work with DHHR to determine the appropriate time to best interact with the West Virginia stakeholders (Home Health and other agencies tasked with providing services and Medicaid Waiver Participants). We will tailor the Training and Outreach Plan to best accommodate your Medicaid participants (Members and Legal Representatives), Provider Agencies, Direct Care Workers, Department staff, and other stakeholders.		
TN007	The Vendor should provide training at the time of registration.	Training
FDGS provides the Department, its stakeholders, provider agencies, and beneficiaries multiple training options. The Training Lead will work with DHHR to identify the appropriate training option for those user types as they register as new users of AuthentiCare. Most on-site, face-to-face training is done with existing staff and users, so we provide additional on-demand training		

Req. ID #	Requirement Text	Requirement Type

capabilities as new users register to use AuthentiCare, including webinars and our detailed AuthentiCare User Manual specific for the West Virginia implementation. We will record the initial training courses and provide the training recordings and associated training material files in formats that are readily available without the need for additional software licenses. On-going training methods include:

- **Webinars:** Subsequent webinars for process reinforcement and for AuthentiCare enhancements offer provider convenience by using a conference call and online format. The advantage for trainees is the ability to sit at one's own computer with the opportunity to ask questions in real time. FDGS uses quality training materials and experienced trainers who are knowledgeable in AuthentiCare for each session. FDGS offers a variety of different times and dates from which providers may choose in order to attend training and still meet their business needs.
- **Provider forums/assistance calls:** The Account Manager, or designated Subject Matter Expert, leads the forums in person or online. Forums allow training of enhancements and offer the community of providers an opportunity to brainstorm among themselves any suggestions they might have to coordinate AuthentiCare with their business needs. These meetings are scheduled regularly to meet provider needs over the time the EVV solution is in place. Once implementation is complete, monthly provider support calls via conference call or webinar can provide ongoing opportunities for questions, continuing education, and identification of areas where clarification may be needed.

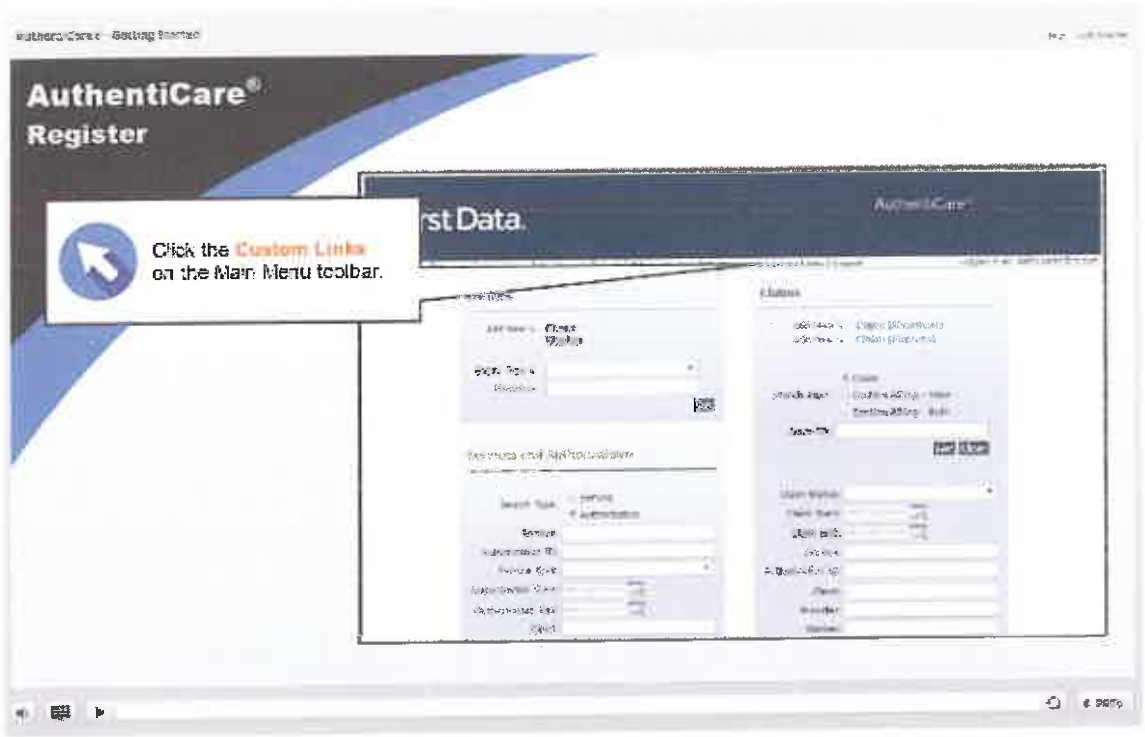


Figure 8.1 – AuthentiCare includes self-paced, web-based training modules available for providers to complete guided click-through scenarios on demand

- **Online web-based training:** FDGS has self-paced, web-based training modules available for providers to review different scenarios on demand. These modules can be used as initial online training or as follow-up training to refresh knowledge and skills. AuthentiCare users may start with any module and move from one module to another at their own pace. The table of contents in each module is designed for forward and backward movement from one topic to another to meet user education needs. The AuthentiCare eLearning environment reinforces the information found in the AuthentiCare User Manual and is part of our collection of training opportunities.
- **AuthentiCare User Manual:** The training materials in the AuthentiCare User Manual will be tailored to West Virginia's EVV programs. This is a comprehensive user manual that documents and explains system functionality. The advantage is an organic document, regularly updated and accessible and searchable online, that reflects changes and enhancements to AuthentiCare functionality. The AuthentiCare User Manual will be updated to reflect

Req. ID #	Requirement Text	Requirement Type
enhancements and other system changes identified during design sessions as well as future changes.		
TN008	The Vendor should collaborate with the Department and the stakeholder community to develop strategies to train members receiving services.	Training
FDGS will work with the Department and its stakeholder community early in the EVV project to review the training and outreach documentation for all user types, including members receiving services and their representatives. Early collaboration with the Department and its stakeholder community is the best way to validate that our training methods will meet the unique needs of the AuthentiCare user base in West Virginia. The Training Lead will use the feedback from the Department and stakeholders to update and finalize the training strategies and methods for each of the different user types within the Training and Outreach Plan, including members receiving services and their representatives.		
TN009	The Vendor should provide both web-based and ten (10) state-wide in-person trainings to users prior to the initial implementation of the solution based on a schedule and locations as agreed upon by the Department.	Training
FDGS offers multiple options for Training and Outreach to meet the EVV training requirements. The Training Lead will work with DHHR to identify the location for the 10 in-person training sessions and to finalize the training schedule for the approved locations to provide statewide training opportunities. We understand that some larger cities may have more than one in-person session to handle larger attendee volumes. For web-based training, FDGS will offer webinars on a variety of different times and dates from which providers may choose in order to attend training and still meet their business needs.		
TN010	The Vendor should provide written training materials for both in-person and web-based training options.	Training
The Training Lead will finalize the AuthentiCare User Guide prior to Go-Live and any major system enhancements. The AuthentiCare User Manual, tailored to DHHR EVV programs, is the key piece of our training materials. This is a comprehensive user manual that documents and explains system functionality. The AuthentiCare team regularly updates the User Manual and makes it accessible and searchable online to reflect changes and enhancements to AuthentiCare functionality. The AuthentiCare User Manual will also be updated to reflect enhancements and other system changes identified during iterative design sessions or other customizations identified later in the project. FDGS will establish and distribute an electronic, Department-approved AuthentiCare User Manual. At a minimum, the User Manual will be updated and distributed annually to all solution users. When major system upgrades occur, the User Manual will be updated to reflect the changes no fewer than seven business days prior to implementation. FDGS captures the EVV policy and procedures within our AuthentiCare User Manual. We will tailor and submit for approval an electronic, Department-approved AuthentiCare User Manual with specific details for West Virginia's EVV. Newly approved and on-boarded providers who did not participate in the initial on-site train-the-trainer training sessions will be provided with direction on how to access the AuthentiCare User Manual and other supplemental training aids. This provides directions to all users to the current version of the EVV policy and procedures.		
TN011	The Vendor should submit all training materials to the Department for review and approval at least 45 calendar days prior to the date of the first training session.	Training
FDGS agrees to provide all training materials to the Department for review and approval at least 45 calendar days prior to the date of the first training session. Depending on the audience, this may result in multiple walkthroughs and submissions for the different training materials used in the different sessions.		
TN012	The Vendor should provide training materials offered in accessible formats consistent with requirements of the Americans with Disabilities Act (ADA) throughout the life of the solution. (Reference: https://www.ada.gov/regs2010/titleII_2010/titleII_2010_regulations.pdf)	Training
The AuthentiCare User Manual and related training materials are consistent with the requirements of the Americans with Disabilities Act (ADA). Our training materials and related documentation also take into account the low literacy levels of that may use AuthentiCare. In other states, we have provided materials at a fourth or fifth grade literacy level to provide for easy understanding and comprehension of the needed EVV features and functions. By remaining consistent with ADA guidelines, for example, end users are able to use screen readers or magnifiers to support special needs due to a visual disability. During the Train-the-Trainer sessions (face-to-face), the Department may provide a sign language interpreter to support those that are hearing impaired.		

Req. ID #	Requirement Text	Requirement Type
TN013	The Vendor should provide training materials and training courses that are accessible for users who do not speak, read, or write the English language, upon request by the Department according tohttps://www.hhs.gov/civil-rights/for-individuals/section-1557/translated-resources/index.html.	Training
FDGS can provide an AuthentiCare User Manual and other training documents in English and Spanish. If additional languages are needed, FDGS will work with the Department to identify the languages required and the associated translation effort.		
TN014	The Vendor should obtain independent verification of the accuracy of all translations made pursuant to language and accessibility requirements.	Training
For Spanish, and mutually agreed upon future translations, FDGS agrees to obtain independent verification of the accuracy of each language.		
TN015	The Vendor should provide web-based training available to users throughout the life of the solution.	Training
For web-based training, FDGS offers the online AuthentiCare User Manual and related training materials, recorded training sessions, and our ongoing training methods including: • **Webinars:** Subsequent webinars for process reinforcement and for AuthentiCare enhancements offer providers convenience by using a conference call and online format. The advantage for trainees is the ability to sit at one's own computer with the opportunity to ask questions in real time. FDGS uses quality training materials and experienced trainers who are knowledgeable in AuthentiCare for each session. FDGS offers a variety of different times and dates from which providers may choose in order to attend training and still meet their business needs. • **Provider forums/assistance calls:** The Account Executive, or designated Subject Matter Expert, leads the forums in person or online. Forums allow training of enhancements and offer the provider community an opportunity to brainstorm among themselves any suggestions they might have to coordinate AuthentiCare with their business needs. These meetings are scheduled regularly to meet provider needs while the EVV solution is in place. Once implementation is complete, monthly provider support calls via conference call or webinar can provide ongoing opportunities for questions, continuing education, and identification of areas where clarification may be needed. • **Online web-based training:** AuthentiCare includes self-paced, web-based training modules available for providers to review different scenarios on demand. These modules can serve as initial online training or as follow-up training to refresh knowledge and skills. AuthentiCare users may start with any module and move from one module to another at their own pace. The table of contents in each module is designed for forward and backward movement from one topic to another to meet user education needs. The AuthentiCare eLearning environment reinforces the information found in the AuthentiCare User Manual and is part of our collection of training opportunities.		
TN016	The Vendor should provide a detailed approach to user training with respect to solution modifications.	Training
FDGS examines each enhancement included in AuthentiCare releases and determines the impact to the training materials and content, including the AuthentiCare User Manual. Besides Release Notes, FDGS maintains system and user documentation to synchronize with functionality updates. The AuthentiCare User Manual will also be updated to reflect enhancements and other system changes identified during the iterative design sessions or other customizations identified later in the project. FDGS will establish and distribute an electronic, Department-approved AuthentiCare User Manual. At a minimum, the User Manual will be updated and distributed annually to all solution users. When major system upgrades occur, the User Manual will be updated to reflect the changes prior to implementation.		
TN017	The solution should maintain a record of all user training, including the name of the individual trained, the date of training, the specific training completed, and whether the training was in-person or web-based.	Training
FDGS will track each user on the day of on-site user training. Our self-paced, web-based e-learning system will record each user that logs into the training system, including the name of the individual trained, the date of training, the training module completed, and training mode (online vs in-person). We can track each user on the provider page and we can send this in the Monthly Scorecard.		
TN018	The Vendor's training records should be included in the data available for reporting.	Training
Our self-paced, web-based e-learning system will record each user that logs into the training system, including the name of the individual trained, the date of training, the training module completed, and training mode (online vs in-		

Req. ID #	Requirement Text	Requirement Type
person).FDGS will maintain all training records and provide the approved training reporting summary in the Monthly Scorecard or to the Department upon request.		
TN019	The Vendor should provide a user manual to all users.	Training
The Training Lead will finalize the AuthentiCare User Guide prior to Go-Live and any major system enhancements. The AuthentiCare User Manual, tailored to DHHR EVV programs, is the key piece of our training materials. This is a comprehensive user manual that documents and explains system functionality. The AuthentiCare team regularly updates the User Manual and makes it accessible and searchable online to reflect changes and enhancements to AuthentiCare functionality. We also update the AuthentiCare User Manual to reflect enhancements and other system changes identified during iterative design sessions or other customizations identified later in the project. FDGS will establish and distribute an electronic, Department-approved AuthentiCare User Manual. At a minimum, the User Manual will be updated and distributed annually to all solution users. When major system upgrades occur, the User Manual will be updated to reflect the changes no less than seven business days prior to implementation. FDGS captures the EVV policy and procedures within our AuthentiCare User Manual. We will tailor and submit for approval an electronic Department-approved AuthentiCare User Manual with specific details for West Virginia's EVV. Newly approved and on-boarded providers that did not participate in the initial on-site train-the-trainer training sessions will be provided with direction on how to access the AuthentiCare User Manual and other supplemental training aids. This provides directions to all users to the current version of the EVV policy and procedures.		
TN020	The user manual should be subject to Department approval.	Training
FDGS agrees to submit the West Virginia-specific AuthentiCare User Manual to the Department for review and approval.		
TN021	The user manual should be available online and in hard copy upon request of the user.	Training
The AuthentiCare User Manual for West Virginia will be available online and as a PDF version for download or print.		
TN022	The user manual should be offered in accessible formats consistent with requirements of the Americans with Disabilities Act. (Reference: https://www.ada.gov/regs2010/titleII_2010/titleII_2010_regulations.pdf)	Training
The AuthentiCare User Manual and related training materials are consistent with the requirements of the Americans with Disabilities Act (ADA). Our training materials and related documentation also take into account low literacy levels of members or providers that may use AuthentiCare. In other states, we have provided materials at a fourth of fifth grade literacy level to provide for easy understanding and comprehension of the needed EVV features and functions. By remaining consistent with ADA guidelines, for example, end users are able to use screen readers or magnifiers to support special needs due to a visual disability. During the Train-the-Trainer sessions (face-to-face), the Department may provide a sign language interpreter to support those that are hearing impaired.		
TN023	The user manual should be available in at least those languages the Department is required to accommodate, in addition to English, pursuant to 45 Code of Regulations (CFR) Section 80.3(b)(2) (Reference: https://www.hhs.gov/civil-rights/for-individuals/section-1557/translated-resources/index.html)	Training
FDGS can provide an AuthentiCare User Manual and other training documents in English and Spanish. If additional languages are needed, FDGS will work with the Department to identify the languages required and the associated translation effort.		
TN024	The solution should support workforce security awareness through such methods including, but not limited to:	Training
TN025	Security reminders (at login or screen access)	Training
TN026	Training reminders	Training
TN027	Online training capabilities	Training

Req. ID #	Requirement Text	Requirement Type
TN028	Training tracking	Training
TN029	Others as defined by the Department.	Training
AuthentiCare is able to display security reminders during registration or include Department-approved reminders using a standard "banner" at login. FDGS will review the Training and Outreach Plan with the Department to identify training materials that should include workforce security awareness content.		

8.5 CMS Certification

RFP Section Attachment 9 – 6, 4.4.3.3, pp. 134, 54
6.1 The Vendor's proposal should describe in detail the Vendor's experience with CMS Certification including the MECT, and a proposed approach to certification of the solution.
6.2 In addition, describe the Vendor's experience in projects subjected to IV&V oversight, the approach to interaction with an IV&V team, and responding to IV&V findings.

Approach to CMS Certification

This sub-section describes our approach to CMS Certification. Our experience includes the detailed use of the Medicaid Enterprise Certification Toolkit and the newly released CMS EVV Outcomes Based Certification (OBC). Addendum 6 to this RFP specifically indicates that DHHR will follow OBC guidance for CMS certification with respect to its EVV solution:

"As described in CMCS Information Bulletin dated October 24, 2019, DHHR will use Outcomes-based Certification (OBC) for the EVV project. References to certification pertain to current and future requirements for EVV as outlined by the most current guidance from CMS."

FDGS provides additional detail in this sub-section to meet the mandatory requirements listed in Table 6.1 as part of RFP Attachment 6 – Mandatory Requirements.

Table 8.4 – AuthentiCare meets all mandatory requirements for CMS Certification

Met	Req ID #	Requirement Text
☑	**MR022**	The Vendor must remain in alignment with all future updates to Centers for Medicare & Medicaid Services' (CMS') certification processes and any future updates to the Medicaid Enterprise Certification Toolkit (MECT) (Reference: https://www.medicaid.gov/medicaid/data-and-systems/mect/index.html)
☑	**MR023**	The Vendor must design the solution to support the Medicaid Information Technology Architecture (MITA) goals for the Department as defined in the Department's MITA State Self-Assessment (SS-A) and other West Virginia MITA artifacts provided in the WV EVV RFP Procurement Library.
☑	**MR024**	The Vendor must coordinate with the Department to develop all documentation required by Centers for Medicare & Medicaid Services' (CMS') Certification process as defined in the most recent Medicaid Enterprise Certification Toolkit (MECT). (Reference: https://www.medicaid.gov/medicaid/data-and-systems/mect/index.html)

In Addendum 6, issued February 25, 2020, DHHR responses to Q011, Q107, and Q124 indicate that DHHR will use Outcomes Based Certification (OBC) for the EVV project. FDGS offers the Department hands-on experience with CMS OBC processes and EVV Certification Criteria and Evidence. From our work with CMS in other states specific to EVV OBC, we know the requirements, the evidence criteria, and the timing of submission for OBC to complete the CMS mandatory Operations Readiness Review (ORR) prior to go live and the preparation post go-live to complete the CMS final certification review and approval.

The Outcomes Based Certification has significant differences in approach from the former MECL process—focus on outcomes measurements and benefits, and a pre go-live focus on functionality, security and privacy risk assessment. The other major difference with OBC is the continual demonstration of outcomes and key performance indicators to continue receiving Maintenance and Operations Federal Financial Participation (FFP) enhanced funding. Unlike

MECL where you receive one certification approval, OBC is a continuous process with quarterly and annual security and privacy reporting to CMS.

Our experience working with other states and CMS allows FDGS the ability to verify that the AuthentiCare EVV solution will meet all mandatory requirements for CMS Certification listed in Table 6.1 above.

To remain in alignment with all future updates to Centers for Medicare & Medicaid Services' (CMS') certification processes, our Subject Matter Experts have been engaged with CMS and our customers through the finalization and implementation of the new EVV Outcomes-Based Certification process and related guidelines. Our approach to CMS Certification for DHHR will be through active participation during DDI, implementation rollout, post-go-live evidence, reporting requirements, and finally CMS Certification.

Outcomes Based Certification Experience

With FDGS, West Virginia DHHR gains the capabilities of our government consulting practice along with our healthcare industry leadership. CMS considers the FDGS EVV solution to be a Medicaid enterprise module and a candidate for certification. FDGS has been working with CMS prior to the official release of the new EVV OBC certification process and guidelines in October 2019. Nevada is one of the first states to be actively pursuing Outcomes Based Certification for EVV. We meet with CMS regularly to ask questions, clarify, and validate OBC release 1.0 requirements, with final certification anticipated the summer of 2020.

Our experience in Nevada and with two other states starting the OBC process will allow us to provide the Department with our knowledge and experience navigating and completing the new EVV OBC process. We will have completed Operations Readiness Reviews with required criteria evidence submissions and review process, the new requirements for Key Performance Indicators and their reporting, and demonstration of functionality in the final certification review for a successful CMS certification approval.

Providing Perspective through IV&V Experience

In addition to our EVV product and program expertise, FDGS is currently working through the new OBC process as the independent verification and validation (IV&V) vendor for our customer in Nebraska. This knowledge and experience from both the solution and IV&V perspectives expands our understanding of the CMS certification process, quality evidence, and timely delivery contributes to a successful go-live to final certification.

Subject Matter Expertise: The CMS Certification SME

FDGS assigns a CMS Certification SME to our AuthentiCare projects as an integral member of the delivery team. Our Certification SMEs have extensive knowledge of CMS certification processes, Medicaid Enterprise Systems, MITA architecture, and EVV solutions. Our Certification SME will be engaged in the West Virginia EVV project from project initiation through to final CMS Certification approval, working with DHHR as an integral member of the AuthentiCare delivery team. At project initiation, the Certification SME will:

- Review the current CMS, HIPAA, NIST, and other mandated requirements that may impact the scope, configuration, and implementation
- Participate in design and delivery, including MECL Requirement/Design Reviews, as applicable

- Prepare for the Operational Readiness Review (ORR) prior to Go-Live.

Post Go-Live, our Certification SME will continue engaging with the customer and CMS in the delivery of Key Performance Indicator reports and preparation for the final certification review meeting. This proactive approach to CMS EVV OBC supports the necessary timing of evidence delivery under OBC, meeting CMS' requirements for certification. Based on the approved project scope and validated functional and system requirements, including those necessary for CMS Certification, FDGS will correct problems or defects preventing CMS Certification.

Our CMS Certification SME will participate in project and technical meetings, review configuration design and development deliverables, and provide expert guidance and recommendations for addressing risks, issues, mitigations, and changes. They are responsible for verifying that what is being built in DDI will meet the CMS certification requirements and state-specific requirements for areas of security, privacy, data retention and other areas that meet or exceed the CMS and Federal requirements (based on the final Appendix 1 – Detailed Specifications submitted with this FDGS proposal).

The CMS Certification SME will support the project team with the development of the certification-related deliverables. We will continue to monitor updated guidance from CMS as OBC impacts the final composition of these and other documentation required for EVV certification.

CMS Certification throughout the Project Lifecycle

Figure 8.2 shows the timing for required evidence gathering and submission throughout the implementation and post go-live lifecycle based on the new EVV Outcomes Based Certification. FDGS realizes that the preparation and lead time needed before the Operational Readiness Review (ORR) with CMS will impact the available time for DDI activities within the required six-month timeline of the implementation period and go-live schedule. Solution configuration and development completion precedes completing the third-party security and privacy audits, creating certification evidence, and submitting the evidence for the Operational Readiness Review. The CMS Certification SME will review configurations and custom development for alignment with the CMS EVV OBC criteria, preventing potential issues for certification. Our proactive approach to certification, along with previous certification experience, provides a streamlined an approach under the new CMS EVV OBC and the Operations Readiness Review requirements for Go-Live.

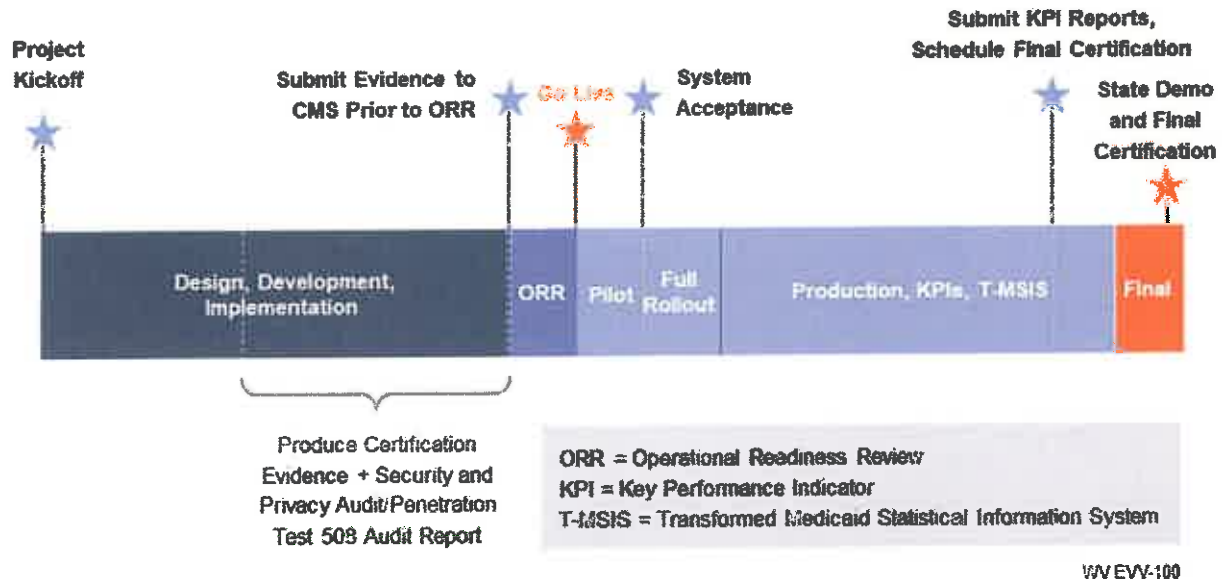


Figure 8.2 – AuthentiCare implementation timeline including CMS certification

Table 8.5 describes the activities of the Certification SME through the life cycle phases and tasks.

Table 8.5 – CMS Certification Activities by Life Cycle Phase

Life Cycle Phase: DDI	Certification SME Activities
Planning	• Review any applicable CMS updates to the Certification process. • If required, provide CMS Certification plan to the State or incorporate into the project schedule. • Work on the procurement schedule and delivery of required SAR and Penetration test audit reports.
Analysis & Design	• Participate in AuthentiCare Design Sessions as a Medicaid SME. • Review state-specific requirements for any exceeding federal standards (data retention, security, privacy, etc.)
Configuration & Development	• Work with the Business Analyst and Test Analyst on scenarios for business function, CMS requirements, and test case development. • Review configuration, integration plan, and customer deliverables.
Testing	• Review test cases and results for the CMS certification scenarios and validation of any state-specific requirements. • Provide the state the CMS certification test results and draft evidence (screenshots for scenarios required) for review and feedback
Training & Outreach	• Validate HIPAA awareness training materials in the various user role type training. Provide handouts for HIPAA awareness at in-person training sessions. • Review preliminary training and outreach reports with the state for format and content feedback. • Collect training and outreach information for later EVV9 Training & Outreach evidence.
Implementation Planning	• Review third-party SAR and penetration test reports. Rectify any certification blocking issues. • Mitigation approaches for certification blocking issues.

Life Cycle Phase: DDI	Certification SME Activities
CMS Operational Readiness Review (Pre Go-Live)	• Produce test reports output and evidence for: EVV1, EVV2, EVV3, EVV4, EVV5, EVV6, EVV7, and EVV9. Provide EVV8 Detailed 508 test report, and EVV10 support for non-native English support. • Submit evidence to the State for review and feedback and submission to CMS. Schedule ORR meeting with CMS, address pre-meeting questions, meeting, close out of any critical items, and track resolution of any non-critical.
Pilot and Roll-out	• Monitor for any major issues that may block system acceptance and start of post go-live production evidence.

Table 8.6 describes CMS Certification SMEs activities during the M&O phase through CMS certification.

Table 8.6 – CMS Certification Activities and Deliverables

Life Cycle Phase: Maintenance & Operations	Certification SME Activities
One Month Post-Go-live	• Review tests of KPI reports Test • Run KPI reports on live data • Review KPI reports for first month including reports that quarterly for verification
System Acceptance/ Production Operations	• Milestone for start of six months post go-live for CMS certification review. • System acceptance letter from Customer (SMA) to FDGS and CMS
CMS Certification Preparation	• Demo preparation, KPI report reviews and submission to CMS, Certification Review meeting request
CMS Certification Review/ approval	• Participate in the prep sessions and the CMS Certification Review Meeting • Completion: CMS Certification approval expected approximately 60 days after close out of review items
Key Performance Indicators and M&O continued compliance	• Develop and submit key performance indicators quarterly for the four functional and availability measures and annually for the security and privacy review KPI. Required for ongoing compliance and enhanced funding M&O.

The CMS Certification SME is an active contributing member of the AuthentiCare delivery team throughout the project. The Certification SME will remain on the project until completion of all CMS Certification deliverables and final CMS Certification.

The AuthentiCare Delivery organization includes a team of experts in CMS policy, MITA, security and privacy, federal standards, and industry best practices who continuously monitor for new requirements, analyze product impacts, and provide input to the AuthentiCare product roadmap. These capabilities provide West Virginia DHHR with the confidence that the EVV System meets federal requirements for certification and enhanced federal funding. Through our CMS certification process, AuthentiCare will support federal reporting requirements as required by the 21st Century Cures Act including the new OBC KPI requirements. CMS Certification is not just a one-time event; maintaining certification is an ongoing process. FDGS recognizes that the quarterly KPI reporting and the annual KPI for a security and privacy review are mandatory to continue receiving the Maintenance and Operations enhanced funding. The FDGS AuthentiCare team is looking forward to support West Virginia DHHR to maintain their enhanced federal funding.

Experience with IV&V

FDGS agrees to support the Department and its contractors, whether IV&V, or other Systems Integrators, to coordinate activities to provide a successful AuthentiCare implementation and achievement of CMS Certification.

The Nevada implementation is one of the first under the CMS Outcomes-Based Certification process. As in Nevada, we anticipate that IV&V for West Virginia will continue to participate in an active role for all meetings as part of the customer's team and represent CMS' interests in a successful project implementation and certification.

Please note that in the new CMS Outcome Based Certification process, IV&V's role is focused on project oversight and has fewer responsibilities for the preparation and review of evidence and does not provide a final report for submission to CMS. As we move forward with the OBC process, FDGS will support the Department and its IV&V contractor throughout the EVV project.

9.0 Attachment 10: Maintenance & Operations Specifications Approach

RFP Section 5.4.2.10 (Table 11) & Attachment 10, & 4.4.3.4, pp. 74, 135, 55
Maintenance and Operations specifications ensure that the solution is fully functional and performing optimally until the end of the lifecycle.
1.1 The Vendor's response should include a narrative overview describing its approach to maintenance of its proposed solution, including updates to new versions of the underlying commercial off-the-shelf (COTS) products, and to configurations necessary to support changes in Department of Health and Human Resources (DHHR's) business needs. Use the response sections to provide specific details of the proposed approach to meeting the maintenance and operations specifications in each subject matter area.
1.2 Responses should reference specifications and relevant mandatory requirements using the appropriate identifications (IDs) from Appendix 1: Detailed Specifications and Attachment 6: Mandatory Requirements. DHHR also expects the Vendor to propose its approach for meeting any narrative in Section 4: Project Specifications of this request for proposal (RFP).

9.1 Operations

RFP Section Attachment 10 – 2, & 4.4.3.4.1, pp. 135, 56
Refer to the relevant maintenance and operations specifications located in Appendix 1: Detailed Specifications and pertinent narrative in Section 4: Project Specifications in this RFP to cover solution capabilities in this area.
2.1 The Vendor should describe its approach to Operations below. The narrative response for this category should be organized using the appropriate subject matter area as per Appendix 1: Detailed Specifications.

FDGS provides ongoing operations and support to our customers through a consistent model to maintain their success as well as ours.

This sub-section describes our approach to Maintenance and Operations. AuthentiCare has now been deployed statewide in Oklahoma, Kansas, New Mexico, Nevada, Alabama, and Texas, as well as continued operations in South Carolina and at WJB Dorn VA Medical Center, which means we have tested our Maintenance and Operations strategy in multiple states and we can bring West Virginia a very effective approach.

Transition to Operations

During the agreed cutover period, the AuthentiCare implementation team will transition the system to our Service Delivery team for ongoing customer service support. A post-implementation review is performed to verify that all requirements have been met and results from the Lessons Learned session are formally documented. Upon successful completion of the cutover, the Project Manager will begin the closeout activities of the implementation project and receive final acceptance from DHHR to begin the Maintenance and Operations phase.

As we described previously in Hardware and Infrastructure requirement IN028, our Help Desk approach fully supports the RFP requirements for Maintenance and Operations. The AuthentiCare Help Desk is easily accessible via email and telephone and is committed to being our customers' valued business partner in support of all FDGS products and services. Our Help Desk makes sure that compliance with our customer's requirements are in place and that responses are provided within the agreed upon timeframes. Support representatives are cross-trained to provide full coverage and are available 24 hours a day, 7 days a week.

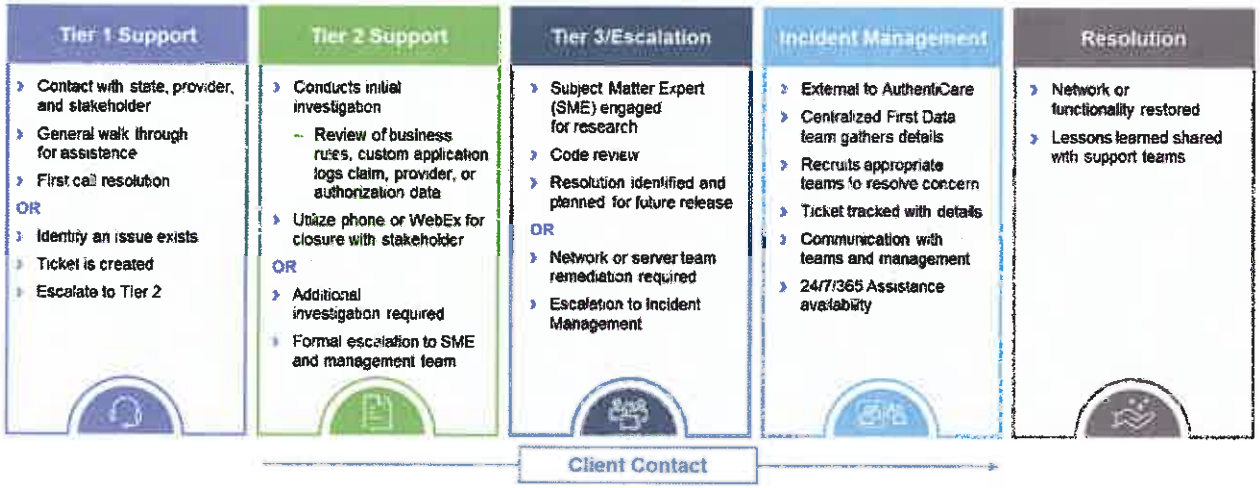


Figure 9.1 – FDGS offers a tiered approach to client support and services

System Maintenance and Release Planning

Once AuthentiCare is transitioned to Maintenance and Operations, FDGS provides a release schedule that will be communicated to the Department and updated in our monthly operations status report. Generally, AuthentiCare provides quarterly releases. High-priority releases due to security concerns or similar will be addressed with DHHR leadership for an emergency update to be scheduled as soon as possible.

As we noted in Project Management requirement PM010, the FDGS team agrees to provide a clear schedule of patching dates and product releases in advance of future system changes. For example, the 2020 patches to AuthentiCare are already planned for the third Saturday of each month, and planned production code release events for 2020 are scheduled quarterly at the end of the month between the hours of 7 PM on Wednesday through 3 AM Central on Thursday. Future schedules of ongoing patches and product releases will be communicated to the Department well in advance of the next promotion date.

As with all AuthentiCare enhancements, FDGS will communicate pending releases that include security patches for software or firmware. We follow a consistent migration path for all changes through Development and QA environments prior to the implementation into the Production environment.

In some instances, major vulnerabilities must be completed in an expedited fashion to close the risk. FDGS will notify the Department following emergency patches and promotion to production.

FDGS provides additional detail to the Operations Subject Matter Area requirements in Table 9.1.

Table 9.1 – Detailed Response to Operations Requirements

Req. ID #	Requirement Text	Requirement Type
OP001	The Vendor should track, and provide the Department access to, process metrics and other detail as defined in the approved Change Management Plan, including, but not limited to:	Operations
OP002	The estimated and actual hours allocated to each change request	Operations
OP003	Specific personnel assigned to each change request	Operations
OP004	Scheduled completion date for each change request	Operations
OP005	Total cost if the maximum allowed hours are exceeded on any approved change request	Operations
OP006	Any change to current operational costs	Operations
OP007	A separate total for equipment requirements (if applicable) related to the modification	Operations
OP008	Others as defined by the Department	Operations
The FDGS Project Manager will capture, manage, and track the required data items related to the Change Management process and the detailed change requests. The Change Request Log will contain all data elements included in OP002 – OP008 plus others that are determined necessary to prioritize change requests that may impact the implementation period or enhancements during the Operations portion of the contract.		
OP009	The Vendor should assure all production software updates, releases, and patches are evaluated and approved by the Department prior to implementation as defined in the Change Management Plan.	Operations
The AuthentiCare Account Manager (and Operations Manager) will communicate with DHHR as software updates, patches, and releases are available on an agreed-upon schedule. Normal AuthentiCare releases are planned quarterly to allow for planning and User Acceptance Testing, if applicable. This provides the Department with advanced notice of regular releases. As a SaaS offering, AuthentiCare provides all of our clients the ability to receive all vetted updates through a consistent release schedule. Once tested and deployed, common functionality is then available to all AuthentiCare customers. System enhancements are typically configurable so features can be selectively enabled. However, there may be instances where FDGS must install an "emergency" update or patch based on a critical fix or other system risk. If an "emergency" install is required, FDGS will notify all of our customers, including DHHR, according to the notification requirements and service levels of the approved Change Management Plan.		
OP010	The Vendor should send notification to the Department when releases are available to be evaluated as defined in the Change Management Plan.	Operations
FDGS provides a release schedule that we communicate to the Department. We provide scheduled updates in our monthly operations status report. Generally, AuthentiCare provides quarterly releases with the appropriate release notes. FDGS agrees to notify the DHHR of any releases that fall outside the previously published release schedule.		
OP011	The Vendor should provide the Department with detailed documentation that provides all fixes and functionality for each release.	Operations
When fixes and functionality updates are released to the production environment, providers and DHHR staff will be provided release notes documenting the change(s), type of change(s) (enhancement, bug fix), the impact, and when appropriate, web-based training to walkthrough the release changes.		
OP012	The Vendor should maintain version control and provide the Department with current system and user documentation.	Operations
The West Virginia AuthentiCare User Manual and impacted system documentation will be updated using version control appropriately to remain current with major releases. All documentation will be provided to the Department according to the approved Change Management Plan and Release Schedule.		
OP013	The Vendor should perform all maintenance and product upgrades for all operational and test environments and hardware at no additional cost so that the system is operating on currently supported version of each product and maintain software and security patches, based on a schedule	Operations

Req. ID #	Requirement Text	Requirement Type
	approved by the Department.	
As a fully hosted solution, we upgrade AuthentiCare's testing and operational components at no additional cost to our customers. Our data centers continually monitor hardware and software within the supported applications for end-of-life planning. The AuthentiCare application is running on currently supported versions across all components. New versions are thoroughly regression tested before inclusion in a future product release to our customers. Product upgrades are included in the Release Notes. FDGS cannot allow the Department to approve our application upgrade schedule. As noted in OP009, FDGS will provide a schedule to the Department for all planned releases, but emergency updates especially those around security will be completed as required by our Cyber Security teams.		
OP014	The solution should provide the ability for the provider agency to review billing prior to submitting for payment.	Operations
AuthentiCare reduces fraud, waste, and abuse by subjecting every visit to a pre-billing claim engine workflow that applies exceptions and prevents providers from billing for incomplete or unauthorized services, preventing compliance issues before they occur. AuthentiCare examines the visit documentation according to configurable business rules and may create one of two types of exceptions: • **Critical Exceptions:** Issues like missing a check-out or missing an authorization are critical and prevent a claim from being billed. • **Informational Exceptions:** Issues like care occurred in an unauthorized location that are flagged for reporting and investigation, but not usually used to prevent billing. Claims with critical exceptions are held in the system for the provider to review and correct, while claims with no exceptions or only informational exceptions are staged for provider approval. AuthentiCare makes it easy for providers to address errors and exceptions that do occur. The system provides an Exception Dashboard that breaks critical exception claims (claims that are currently non-billable) into separate categories for any date of service range. Clicking on a list button takes the provider to a summary list of claims with that exception for the provider to drill down and make corrections. The workflow and its administrative web applications allow FDGS to configure business rule options according to DHHR policies to control how claims are verified and exceptions are applied. This in turn determines how claims are ultimately billed. Working with our customers and their waiver and non-waiver rules, FDGS has built a library of configurable workflow plug-ins that encompass the most common Medicaid business rules for processing visits.		
OP015	The solution should provide the ability for the provider agency to review and correct billing errors prior to submission.	Operations
In addition to the process described in OP014, manually entered edits, corrections, and overrides are performed in an AuthentiCare web process where specific authorized users can make corrections, and, for some types of edits, specific users are empowered to approve or deny them before billing can take place. AuthentiCare supports requiring a reason code for reporting and visit note for added or edited services. The system also provides a full audit trail of changes made including date, time, user ID, and a record of the change. AuthentiCare supports the ability for a provider to add notes and text explanations. The Claim History report includes more details of edits and changes and supports viewing of notes added to each record.		
OP016	The solution should provide the Department and provider agencies with reports of unbilled encounters through front-end edits including, but not limited to:	Operations
OP017	No authorization	Operations
OP018	Expired authorization	Operations
OP019	Reasons that prevented claims from filing	Operations
OP020	Edits made to claims	Operations
OP021	Others as defined by the Department	Operations

Req. ID #	Requirement Text	Requirement Type
AuthentiCare makes it easy for providers to address errors and exceptions that do occur. The system provides an Exception Dashboard that breaks critical exception claims (claims that are currently non-billable) into separate categories for any date of service range. Clicking on a list button takes the provider to a summary list of claims with that exception for the provider to drill down and make corrections. The Exception Dashboard will support those items noted in OP017 – OP020. Additional exception criteria will be discussed in the iterative design sessions. The workflow and its administrative web applications allow FDGS to configure business rule options according to DHHR policy to control how claims are verified and exceptions are applied. This in turn determines how claims are ultimately billed. Working with our customers and their waiver and non-waiver rules, AuthentiCare maintains a library of configurable workflow plug-ins that encompass the most common Medicaid business rules for processing visits.		
OP022	The Vendor should provide a report of all daily transactions, including interactions via the call center, available to the Department in a variety of formats, including, but not limited to:	Operations
OP023	Browser-based	Operations
OP024	Portable Document Format (PDF)	Operations
OP025	Excel	Operations
OP026	Comma-Separated Value (CSV)	Operations
OP027	Others as defined by the Department	Operations
FDGS agrees to provide the Department a report of all daily transactions, including interactions via the call center. Daily reports are currently available in standard formats including PDF, Excel, and CSV. If necessary, the existing formats can be ported directly to a generic htm/html file for display in a web browser. The monthly operations status report contains summary call center statistics and can be provided to the Department in either Word or PDF format.		
OP028	The solution should track metrics for each type of correspondence generated in the solution.	Operations
AuthentiCare does not support automated correspondence nor related metric reporting specific to generated correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
OP029	The solution should track the status of notices that are moving through the generation process.	Operations
Providers, Payers, and Case Managers can use the AuthentiCare web application to see late and missed visit notices and status in real time. They can also see the same information in real time by running and viewing on-demand late and missed visit reports.		
OP030	The solution should notify the Department when an undelivered scheduled system-generated correspondence is approaching the predetermined delivery timeframe as agreed upon by the Department.	Operations
AuthentiCare does not support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
OP031	The solution should have the ability to track when any correspondence or form has been reissued or revised as agreed upon by the Department.	Operations
AuthentiCare does not support automated generation of forms or correspondence. With our focus on establishing Cures Act compliance and CMS certification for West Virginia's EVV solution in Phase 1, FDGS will work with the Department to address future features and functions as AuthentiCare enhancements using the T&M funding quoted in the cost response once Phase 1 has been successfully implemented.		
OP032	The Vendor should pay and arrange for an annual Statement on Standards for Attestation Engagements, System, and Organization Controls (SOC) 1, Type II audit, using the most current version of the audit, which should cover work performed by the Vendor at the Vendor's facility and data center sites. (Reference: https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20	Operations

Req. ID #	Requirement Text	Requirement Type
	by%20the%20CTO/2019/PO1008_Audit_Mar2019.pdf)	
FDGS acquires an annual SOC 1, Type II audit annually for AuthentiCare. The SOC 1 covers work performed by the FDGS/Fiserv at our facilities and data center sites.		
OP033	The Vendor should submit the annual Statement on Standards for Attestation Engagements, System, and Organization Controls (SOC) 1, Type II audit report, using the most current version of the audit, to the Department for approval with an action plan to remediate findings within a timeframe agreed upon by the Vendor and the Department.	Operations
FDGS agrees to provide an external customer summary of the SOC 1 report including the audit findings and the associated management action plan. However, FDGS cannot agree to the Department's request to approve the audit report nor the timeframe or action plan for FDGS to remediate the audit findings. FDGS provides EVV services in a multi-tenant client services environment. As a result, FDGS cannot allow for one client to have control over and dictate FDGS' policies and processes that would impact and affect so many of FDGS' other clients. As to the timeframe of the action plan to remediate findings, the findings discovered during the audit will be remediated by FDGS prior to the final distribution of the SOC 1 report. We understand the State's concern to properly address and remediate specific findings, but to provide effective security, FDGS must have a coherent policy approach based on our knowledge and experience with our own processing environment. In a multi-client environment, it would be impossible to follow or adapt to the differing and perhaps conflicting requirements from multiple clients. As an outside company, the State's information Security Policy does not address the specific requirements and needs in the FDGS environment. AuthentiCare is hosted at Fiserv Data Centers. Because these data centers support thousands of clients, we cannot change our IT policies to match one client's policies. We must be able to maintain our strict policies and procedures for all of our customers across our entire processing environment.		
OP034	The solution should archive and store user profiles for a period of time agreed upon by the Department.	Operations
All AuthentiCare data, including user profiles, will be archived and stored for a period of time agreed to with the Department.		
OP035	The Vendor should provide its incident reporting procedures to the Department for review and approval within a timeframe agreed upon by the Department.	Operations
FDGS agrees to share our incident reporting procedures with the Department for review and comment. Because these procedures support multiple clients within our data centers, FDGS agrees to consider all comments regarding the incident reporting procedures.		
OP036	The Vendor should detail the performance metrics and targets used to monitor the effectiveness of technical support by phone.	Operations
AuthentiCare Operations monitors and tracks specific performance metrics and targets for technical support by phone. Metrics are included in the monthly operations status report. FDGS will work with DHHR to identify whether additional performance metrics should be considered to attain approved service levels.		
OP037	The solution should have the ability to provide an immediate response acknowledging all email inquiries and establishing a timeframe for the response.	Operations
Technical issues can be reported through sending an email to AuthentiCare.Support@FirstData.com. Senders will receive an auto-reply to acknowledge the receipt of the email and notify them that the issue will be reviewed within one 24-hour business day. For critical issues, FDGS recommends attempting to contact the Tier 1 Call Center prior to sending an email.		
OP038	The solution should have the ability to resolve all email inquiries to the Vendor's technical support within one 24 hour business day from initial receipt.	Operations
FDGS agrees to respond to all email inquiries within one 24-hour business day from initial receipt. Again, for technical issues, the most efficient manner for resolution is to contact the Tier 1 Call Center.		
OP039	The Vendor should document inquiries and provide the Department with routine reports regarding reasons for technical support requests.	Operations
As your EVV vendor, FDGS will collaborate with DHHR to develop custom dashboards that provide the most important information to the Department's management team. In the Operations Phase of this contract, FDGS will provide SLA and key business and performance tracking in the monthly dashboard, reporting the previous month's performance. All		

Req. ID #	Requirement Text	Requirement Type

inquiries will be documented including the reason for the inquiry and available for reporting to the Department.

We also review project reporting standards and confirm status report templates, along with key reporting resources for all stakeholders. FDGS will produce a Monthly Status Report, which includes a summary of work activities and major accomplishments achieved during the reporting period, in addition to any problems or issues that require management attention. Our AuthentiCare team will work with DHHR to develop the format and distribution channels for the status report. The status report will include an ongoing project dashboard with key metrics. It will also include graphs and tabular data, and provide a monthly view of IVR call volume, claims created via IVR or Mobile application, exported claims, active entities, system uptime, system downtime, SLA tracking, ticket tracking, and help desk call volume. Figure 9.2 shows a sample table of help desk tracking metrics.

AuthentiCare Help Desk Tracking

Client Support Service Level Agreements **Latest Month: June 2019**

2019 AuthentiCare	Report Day	Tickets Recorded 100%	Call Center Answered Call (30 secs or less)	System Uptime%	Technical Support 24x7	General Support 8am to 5pm EST
January	2	Y	85.50%	100.00%	Y	Y
February	1	Y	93.27%	100.00%	Y	Y
March	1	Y	94.68%	100.00%	Y	Y
April	1	Y	96.54%	100.00%	Y	Y
May	1	Y	96.97%	100.00%	Y	Y
June	1	Y	95.00%	100.00%	Y	Y

Figure 9.2 – Sample Help Desk Metrics as part of the Monthly Operations Dashboard

The Monthly Operational Report will contain a summary of any planned updates/upgrades to the system or any planned outages for system maintenance and other data metrics as required by the state.

Transparent reporting of all operational aspects and consistent communication to the Department and its stakeholders provides the best opportunity for providing the best EVV program services to your provider community and beneficiaries.

OP040	The Vendor should document any procedural action that occurred as a result of a complaint to the help desk and submit this documentation to the Department on an agreed upon schedule.	Operations
FDGS agrees to document any procedural action that occurred as a result of a complaint to the help desk and submit this documentation to the Department in the Monthly Operations Status Report or other agreed-upon schedule. The Account Manager or Operations Manager will review the Operations Handbook with specific DHHR staff. This handbook describes how we conduct root-cause analysis (RCA) to identify areas for continuous improvement.		
OP041	The Vendor's Technical Call Center should provide a toll-free voice messaging system that is compliant with the Americans with Disabilities Act (ADA) and supports limited English proficiency as defined by the Department of Health and Human Services (HHS). (References: https://www.ada.gov/regs2010/titleII_2010/titleII_2010_regulations.pdf, https://www.hhs.gov/civil-rights/for-individuals/special-topics/limited-english-proficiency/index.html). The Technical Call Center should function 24 hours per day, 365 days per year, and provides callers information including, but not limited to:	Operations
OP042	Hours of operation	Operations
OP043	Options for leaving messages after hours	Operations
OP044	Options for leaving messages based on queue hold times and designated intervals as defined by the Department	Operations

Req. ID #	Requirement Text	Requirement Type
OP045	Recording of informational messages as defined by the Department	Operations

Our Help Desk approach fully supports the RFP requirements for Operations and Customer Service. The FDGS Help Desk is easily accessible via email and telephone and is committed to being our customers' valued business partner in support of our products and services, making sure compliance with our customer's requirements is in place. Support representatives are cross-trained to provide full coverage and are available 24 hours a day, 7 days a week.

FDGS realizes that problems and technical issues do not limit themselves to normal business hours, which is why a Tier 2 Help Desk Specialist is on call 24x7 to resolve or escalate issues that occur outside of standard business hours. A call to the support number that is outside of standard business hours will be routed to a Tier 2 Help Desk Specialist to support evenings, weekends, and holidays for technical application concerns.

If needed, our help desk is able to support those with limited English proficiency by including translation services. FDGS will work with DHHR support teams as well to modify or define recorded information specific to the West Virginia EVV program. The full IVR decision path will be reviewed with the Department during the iterative design sessions to verify the specific options available to callers.

OP046	The solution should have the ability to record and report on the performance and utilization of resources within the overall system, including, but not limited to:	Operations
OP047	Average speed of answer	Operations
OP048	Interface processing time	Operations
OP049	Request time for report generation	Operations
OP050	Others as defined by the Department	Operations

To support approved service level agreements (SLAs) and key performance indicators (KPIs), the AuthentiCare solution tracks several technical and operational performance measures. These are monitored to address system bottlenecks as well as operational concerns for customer service.

Call center statistics including speed to answer, calls dropped, and resolution time are captured in detail and summarized in the monthly Operations Status Report. Prior to Go-Live and the transition to the Operations phase of the project, FDGS will work with DHHR to verify the appropriate performance metrics are captured and reported.

AuthentiCare also incorporates several performance monitors for tracking interface processing time, report generation time, long-running transactions, and component/system load. We use AppDynamics Performance Monitor (APM), a suite of tools to maintain stability and availability of the AuthentiCare solution platform. APM also allows FDGS to monitor the performance of AuthentiCare's key business functions within the hardware and software infrastructure layers and alerts on critical resources component utilization or when response thresholds are exceeded so that proper action can take place to restore proper functioning and performance of the systems.

AuthentiCare uses proactive log alerting to identify long-running blocking processes. Indexes and partitioning are in place to manage data access without having to remove data from the primary database. Our customer service agents perform their duties using the production transactional database as do external users, including providers and state staff. Reporting is run against a read-only replicated copy of the database to prevent performance risk on the transactional database.

Other performance and utilization reports should be defined and requested by the Department through the approved Change Management process.

OP051	The Vendor should document and maintain technical specifications associated with the solution including, but not limited to:	Operations
OP052	Complete listing of all software, hardware, and configurations that are required to establish fully functional installations in each of the required environments.	Operations
OP053	Complete specifications for all software, environments, and hardware used to support the solution.	Operations
OP054	Others as defined by the Department	Operations

Req. ID #	Requirement Text	Requirement Type
As we implement AuthentiCare for each customer, FDGS must follow stringent procedures defined by our shared data center resources to establish quality assurance, customer acceptance, and production environments. We submit the detailed technical specifications for each environment to be established for the West Virginia EVV project. The technical specifications include the requirements for server processing, database size and storage, based on projected usage provided by DHHR. Our application development teams and operations teams maintain the inventory of all related software, hardware, and configuration details necessary to deploy and operate the multiple AuthentiCare environments for each jurisdiction. FDGS will review the technical specifications with DHHR prior to the establishment of the initial AuthentiCare environment for the West Virginia EVV project.		
OP055	The Vendor should provide the Department with a capacity analysis report for the solution and the hosted environment including, but not limited to:	Operations
OP056	Hardware	Operations
OP057	Environment	Operations
OP058	Network specifications	Operations
OP059	Others as defined by the Department	Operations
AuthentiCare incorporates AppDynamics Performance Monitor (APM), a suite of tools to maintain capacity, stability, and availability of the AuthentiCare solution platform in support of the approved service level agreements (SLAs). APM also allows FDGS to monitor the performance of the key business functions of AuthentiCare within the hardware, software, and network infrastructure layers and alerts on critical resources component utilization or when response thresholds are exceeded so that action can take place to restore proper functioning and performance of the systems. We have real-time data capture and archives used for performance and utilization trending that drives our capacity review and upgrade process. FDGS will use monitoring software to proactively monitor performance and capacity to support DHHR. Components identified for improvement will be reviewed and implemented as necessary to meet or exceed SLAs. Infrastructure monitors on the servers and database continually monitor memory, CPU, and disk usage, along with any system or database server errors. FDGS reviews database performance and maintenance plans regularly to optimize processing performance. The Account Manager or Operations Manager will report regular capacity analysis findings and recommendations through the Monthly Operations Status Report.		
OP060	The solution should provide real-time solution performance data.	Operations
AppDynamics provides both real-time dashboard and drill-down capability for monitoring system transaction activity, transaction times, and defined alert thresholds that help support personnel proactively maintain expected performance levels, including mobile and web service transactions. Figure 9.3 provides a screen shot of a sample dashboard for the AuthentiCare platform's performance.		

Req. ID #	Requirement Text	Requirement Type

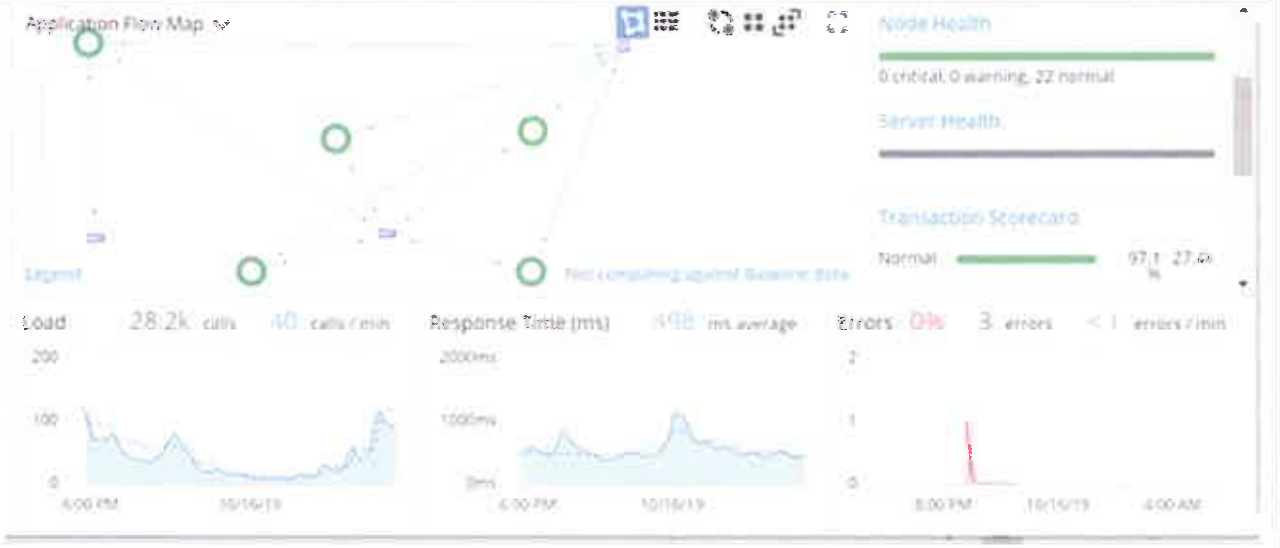


Figure 9.3 – Real-time Application Performance Monitoring of the AuthentiCare application

Our Senior Help Desk Specialists monitor the AuthentiCare daily operating statistics. The Help Desk maintains a checklist of expected processing for the West Virginia EVV project to verify that all processes execute properly. Infrastructure monitors on the servers and database continually monitor memory, CPU, and disk usage, along with server logs. These monitors enable FDGS staff to proactively address system concerns.

OP061	The solution should report on total processing times based on user-defined queries.	Operations
FDGS tracks the total processing time for user-defined queries and will include these statistics with the Monthly Operations Status Report.		
OP062	The solution should write all errors to an error log in a standard format and make it available for Department review upon request.	Operations
AuthentiCare logs errors using a variety of software tools and technical processes. The data captured includes extensive data specific to each error. Generally, our technical analysts use licensed software to further research errors and determine root cause. The raw log data are not normally shared with customers to prevent release of confidential data and its proprietary format.		
OP063	The solution should allow the Department's administrator to view, filter, sort, and search the error log(s).	Operations
Similar to OP062, our technical analysts use licensed software to further research errors and determine root cause. The raw log data are not normally shared with customers to prevent release of confidential data and its proprietary format.		
OP064	The Vendor should notify the Department regarding which releases of third-party software (JAVA virtual machine, Internet Explorer, Mozilla, Safari, etc.) are known to create problems with the current version of the Vendor software.	Operations
FDGS agrees to notify the Department of any hardware or software (or specific versions of software) that may cause conflicts or other known problems with the current release of AuthentiCare and its technical components.		
OP065	The solution should schedule and support file transfers as requested and agreed upon by the Department.	Operations
As an experienced and mature EVV solution, AuthentiCare is skilled in integrating all components of a successful EVV solution, including the transfer of data to and from other systems on a schedule that FDGS and the Department agrees on. The two most common file transfers or interfaces are batch processing (usually daily, but can be executed on a different schedule) and web service exchange (real time). For batch processing, AuthentiCare receives data from provider agencies, support coordinators, the State's fiscal agent, or other external stakeholders daily and processes during a defined timeframe. AuthentiCare receives these imports in an XML format and then imports them into AuthentiCare's databases. Once a file is imported, an import		

Req. ID #	Requirement Text	Requirement Type

results file is created that shows the success or failure of the overall process and lists any error records with the reason for the error. Bulk file exchanges with the state or with MCO trading partners use our File Gateway to transfer files by SFTP. Providers drop and pick up smaller files using a secure web portal. Providers can receive email notification when their files have processed and results are available for pick up.

For web service interaction, the same data elements are transmitted in real time, using secure web services APIs. AuthentiCare uses an industry-standard JavaScript Object Notation/Representational State Transfer (JSON/REST) format. Having data updated in real time improves accuracy and timely reporting, including interactive dashboard updates.

Table 9.2 identifies the standard data transfers that are often required when implementing and updating an EVV solution.

Table 9.2 – Standard Data Updates to and from AuthentiCare

Name	Usual Source	Description
Authorization import	The State or MCOs	Load New/Changed Authorizations from an external system (provider agency, support coordinator, fiscal agent, MMIS system, other state database) to AuthentiCare. This can include the plan of care tasks to be completed. Once a visit is verified, the tasks provided by the attendant can be compared to the plan of care.
Beneficiary Import	The State or MCOs	Load New/Changed Beneficiary (service recipient) enrollment details from an external system (provider agency, support coordinator, fiscal agent, MMIS system, other state database) to AuthentiCare.
Provider Import	The State or MCOs	Load New/Changed Provider enrollment details from an external system (provider agency, support coordinator, fiscal agent, MMIS system, other state database) to AuthentiCare.
Case Manager Import	The State or MCOs	Load New/Changed Case Managers/Care Coordinators' data from an external system (provider agency, support coordinator, fiscal agent, MMIS system, other state database) to AuthentiCare.
837P, 837I Claim Export	AuthentiCare to the State or MCOs	Submit authorized and confirmed claims for EVV services to MCO payers or the state MMIS on behalf of Providers.
835 Payment Files	Providers	Receive 835 payment files from providers, and report on claim payments and denials.
Worker Schedules	Providers	For Providers that have their own scheduling system, FDGS can accept file uploads of worker schedules to input or update schedules in AuthentiCare.
Worker Import	Providers	Providers manage their workers directly through the administrative portal. If a provider requires a complete import of worker data, FDGS can work with them on data elements and formats to submit a full worker upload.

OP066	The solution's data aggregation component should send each provider agency a verified visit report, at least once a calendar day.	Operations

EVV-required data, including visit data from GPS and other alternative location methods, is accepted if provided by external systems and retains an identifier to note from which system the data was captured. As data are aggregated into AuthentiCare, provider reports for verified visits by the billing provider, visits that were not verified, and others are available. To maintain secure access to report data, provider agencies must securely log in to access their respective Reports page to review their reports. AuthentiCare allows reports to be downloaded to PDF, Excel, and CSV formats.

OP067	The solution's data aggregation component should send each provider agency a visit not verified report showing visits that were not verified by the provider agency, at least once each calendar day.	Operations

Similar to OP066, as soon as data are aggregated into AuthentiCare, provider reports for verified visits by the billing provider, visits that were not verified, and others are available on demand. To maintain secure access to report data, provider agencies must securely log in to access their respective Reports page to review their reports. AuthentiCare allows reports to be downloaded to PDF, Excel, and CSV formats.

9.2 Solution Backup, Disaster Recovery, and Failover

RFP Section Attachment 10 – 3, & 4.4.3.4.2, pp. 135-136, 56
Refer to the relevant maintenance and operations specifications located in Appendix 1: Detailed Specifications and pertinent narrative in Section 4: Project Specifications in this RFP to cover solution capabilities in this area.
3.1 The Vendor should describe its approach to Solution Backup, Disaster Recovery, and Failover below. The narrative response for this category should be organized using the appropriate subject matter area as per Appendix 1: Detailed Specifications.

This sub-section describes our approach to solution backup, disaster recovery, and failover.

The EVV system will use the AuthentiCare platform within Fiserv's secure and redundant hosted environment. AuthentiCare is hosted in a "Captive Cloud" solution that provides the scalability benefits of a cloud solution. To maximize availability, AuthentiCare operates in parallel data centers in geographically diverse locations with the primary site located in Chandler, Arizona and the secondary site located in Omaha, Nebraska. Full capacity for AuthentiCare is available in both sites. Fiserv maintains fully documented policies and procedures for Disaster Recovery and Business Continuity.

Table 9.3 – AuthentiCare Facility Statistics

Facility Feature	Chandler	Omaha
Raised Floor Square Footage	50,000	60,000
Underground Diesel Fuel Capacity (gallons)	50,000	60,000
Air Conditioning Capacity (tons)	860	1,478
Chilled Water Capacity (tons)	2,000	2,000
Available Electrical Power (megawatts)	10	10
UPS Capacity (kVA redundant)	5,400	5,400

Having a full set of servers in the Disaster Recovery site and replicated data facilitates minimizes service interruption. With this approach, we are already able to meet your short- and long-term restoration, relocation, or replacement of resources for the business continuity requirements, allowing the smooth continuation of operations related to the DHHR EVV system and program data. FDGS understands what our customers need in an emergency situation and our plans incorporate the resources and processes to support communications, supplies, transportation, space, power and environmental controls, documentation, people, data, software, and hardware.

On the AuthentiCare platform, we maintain a two-dimensional backup procedure to eliminate disruption of service or data loss due to system failures or destruction. Full backups are taken daily, at times when user activity is low. In addition, transaction logs are backed up at five minutes to the hour every day. In the event of a database failure, this combination of backups—transaction log and full database—provides the requisite input source to recover the database up to the time that the failure occurred (point-in-time recovery).

In the event of a disruption of service to the primary site, the secondary site assumes processing of the additional workload, allowing users to continue execution of service without outages or delays. As portrayed in Figure 7.13, within Security Management requirement SM143, our redundant data center architecture provides AuthentiCare application and data backups supporting our Disaster Recovery and Business Continuity Plans.

With data center redundancy and real-time transaction replication of data between data centers, most operating contingencies that arise can be mitigated by re-routing data traffic until the issue is resolved.

Data backups collected from the AuthentiCare system are securely stored at geographically dispersed, networked data backup locations spread across Fiserv facilities as an extra safety measure. The backups are encrypted and networked across a distributed storage infrastructure so that the data never leaves a secure Fiserv facility and captive network, but maintains redundancy across facilities, protecting data from loss at any one facility. This eliminates the need for offsite storage using magnetic media that would require secure handling, storage, and sanitization according to NIST SP 800-88.

FDGS provides additional detail to the solution backup, disaster recovery, and failover subject matter area requirements in Table 9.4.

Table 9.4 – Detailed Response to Solution Backup, Disaster Recovery, and Failover Requirements

Req. ID #	Requirement Text	Requirement Type
DR001	The solution should provide sufficient transaction logging and database back-up to allow it to be restored. If multiple databases are used for work item routing and program data, restoring the solution should ensure that databases are synchronized to prevent data corruption.	Solution Back-up, Disaster Recovery, and Failover
On the AuthentiCare platform, we maintain a two-dimensional backup procedure to eliminate disruption of service or data loss due to system failures or destruction. Full backups are taken daily, at times when user activity is low. In addition, transaction logs are backed up at five minutes to the hour every day. In the event of a database failure, this combination of backups—transaction log and full database—provides the requisite input source to recover the database up to the time that the failure occurred (point-in-time recovery). Data backups collected from the AuthentiCare system are securely stored at geographically dispersed, networked data backup locations spread across Fiserv facilities as an extra safety measure. The backups are encrypted and networked across a distributed storage infrastructure so that the data never leaves a secure Fiserv facility and captive network, but maintains redundancy across facilities so data are protected from loss at any one facility. This eliminates the need for offsite storage using magnetic media that would require secure handling, storage, and sanitization according to NIST SP 800-88.		
DR002	The solution should have the ability to perform online backups without interruption to production operations, according to a schedule agreed upon by the Department.	Solution Back-up, Disaster Recovery, and Failover
On the AuthentiCare platform, we maintain a two-dimensional backup procedure to eliminate disruption of service or data loss due to system failures or destruction. Full backups are taken daily, at times when user activity is low. In addition, transaction logs are backed up at five minutes to the hour every day. In the event of a database failure, this combination of backups—transaction log and full database—provides the requisite input source to recover the database up to the time that the failure occurred (point-in-time recovery). FDGS will verify the backup schedule with the Department prior to Go-Live.		
DR003	The solution should allow continued use of the system during back-up and perform back-ups during non-peak processing hours, to minimize the impact to operational activities.	Solution Back-up, Disaster Recovery, and Failover
On the AuthentiCare platform, we maintain a two-dimensional backup procedure to eliminate disruption of service. Full backups are taken daily, at times when user activity is low. In addition, transaction logs are backed up at five minutes to the hour every day.		
DR004	The solution should support data freezing.	Solution Back-up, Disaster Recovery, and Failover
If necessary, AuthentiCare can support data freezing. However, with respect to Solution Back-up, Disaster Recovery, and Failover, data freezing does not apply. The AuthentiCare application runs a configuration of SQL that is Always On, so there is no migration of data necessary to move to or from a Disaster Recovery state. With the Availability Group (AG) client set to Always On, FDGS minimizes the risk to our AuthentiCare clients. We have		

Req. ID #	Requirement Text	Requirement Type
established asynchronous commitment of all database transactions. We also complement our data infrastructure with application layer logging to verify that all data interactions completed successfully.		
DR005	The Vendor should maintain an operational back-up power supply capable of supporting vital functions.	Solution Back-up, Disaster Recovery, and Failover
AuthentiCare is hosted in data centers that include operational back-up power supplies capable of supporting all vital functions. Please see Table 9.3 – AuthentiCare Facility Statistics at the beginning of this sub-section. The data centers hosting AuthentiCare maintain redundant UPS Capacity of 5400 kVA.		
DR006	The Vendor should equip facilities with proper safeguards for fire prevention, fire detection, and fire suppression that are consistent with local fire codes.	Solution Back-up, Disaster Recovery, and Failover
Fiserv's world-class data centers host AuthentiCare and provide for fire prevention, fire detection, and fire suppression consistent with or in excess of local fire codes.		
DR007	The Vendor should equip fire detection and alarm systems with uninterruptable power supply.	Solution Back-up, Disaster Recovery, and Failover
All components, including fire detection and alarm systems, are equipped with uninterruptable power supplies.		
DR008	The Vendor should have a remote backup facility at least one hundred (100) miles away from the primary data center.	Solution Back-up, Disaster Recovery, and Failover
Our primary and backup data center facilities are approximately 1,300 miles apart.		
DR009	The Vendor should conduct an annual disaster recovery exercise at a mutually agreed upon time and provide the results to the designated Department staff. Department staff should be invited to be included in these exercises.	Solution Back-up, Disaster Recovery, and Failover
FDGS/Fiserv conducts annual testing of both the Business Continuity Plan and Disaster Recovery Plan for AuthentiCare. FDGS will work with DHHR and its project leadership to review the current backup and recovery process. If necessary, we can discuss our current test scenarios and any options for different types of backups or dataset reloads as appropriate. The Account Manager will work with DHHR to identify a mutually agreed-upon time based on the full DR test plan schedule for our data centers. We will also identify where Department staff should be included in AuthentiCare recovery testing activities. Once completed, we will compile the test results for review with the Department staff.		
DR010	The Vendor should store all backup copies in a Department-approved backup storage location for a period of time specified by the Department.	Solution Back-up, Disaster Recovery, and Failover
FDGS will work with the Department to verify the data retention period for storage of backup copies. Data backups collected from the AuthentiCare system are securely stored at geographically dispersed networked data backup locations spread across Fiserv facilities as an extra safety measure. The backups are encrypted and networked across a distributed storage infrastructure so that the data never leaves a secure Fiserv facility and captive network, but maintains redundancy across facilities so data are protected from loss at any one facility. This eliminates the need for offsite storage using magnetic media that would require secure handling, storage, and sanitization according to NIST SP 800-88.		

10.0 Appendix 1: Detailed Specifications

RFP Section 5.4.2.10 (Table 11) & Appendix 1, pp. 74 & 137
See the attached Microsoft Excel® file titled, Appendix 1: Detailed Specifications. Review the following instructions:
1.1 The Vendor should self-score each requirement listed in the Capability Assessment column of Tab 3 - Specification & Responses, using only the values that appear in the drop-down list.
1.2 Capability Assessment values are outlined below:
1.2.1 "Will Meet": Vendor agrees to specification.
1.2.2 "Will Not Meet": Vendor declines to meet the specification.
1.3 All specifications should contain one of the values identified above. Any specification without a Capability Assessment response value will be considered to be "Will Not Meet."
1.4 In addition, the Vendor should provide the Attachment, Section, and Page Number(s) where its detailed narrative response for each specification resides, providing the Department of Health and Human Resources (DHHR) with a crosswalk, and ensuring that each specification is addressed. Be advised that the column has been pre-populated with the location that DHHR anticipates the requirement response to reside, however it is up to the Vendor to update that column accordingly should the Vendor respond to a requirement in a different location.
1.5 Hierarchy Level: The hierarchy level column defines relationships between parent and child specifications. DHHR refers to parent specifications as specifications that rely on the content of a subset of related specifications (children) to fully define the scope of the requirement. DHHR refers to child specifications as specifications that rely on additional context provided by a higher-level specification (parent) to fully define the scope of the specification. A hierarchy value of 1 denotes the highest-level specification. Any greater hierarchy value denotes a child specification. For example, a hierarchy level 2 is a child to the nearest prior hierarchy level 1 as illustrated below:
Hierarchy Level 1Specification
↳ Hierarchy Level 2 Specification

FDGS reviewed all requirements listed in Appendix 1: Detailed Specifications. According to the instructions in the RFP, we have completed our Capability Assessment with either Will Meet or Will Not Meet.

For the items that we felt appropriate to mark as Will Not Meet, our AuthentiCare EVV either does not fully meet the requirement at this time or it is not part of our product capabilities at this time. Several of these items are partially supported by AuthentiCare, but to remain fully transparent with the Department, we felt that Will Not Meet was the appropriate assessment. We look forward to working with the Department in identifying priorities for future enhancements as they become more familiar with the robust capabilities of AuthentiCare already in place.

As required, FDGS submits a cross-reference or crosswalk to our proposal by Attachment, Section, and Page Number(s) where the detailed narrative response for each specification resides.

10.1 Completed Appendix 1: Detailed Specifications

The following tab provides the complete Appendix 1: Detailed Specifications with our Capability Assessment.

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
PG001	3994	1	The solution rules/procedures should allow and enforce multiple service limits for different service ranges including, but not limited to:	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-17
PG002	5140	2	Day	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-17
PG003	5141	2	Week	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-17
PG004	5142	2	Month	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-17
PG005	5143	2	Year	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-17
PG006	3995	1	The solution rules/procedures should accommodate retroactive prior authorizations and changes to prior authorizations based on revisions to recipients' plans of care/service plans.	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-17
PG007	4001	1	The solution should have the ability to round service delivery time.	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-18
PG008	4767	1	The solution should provide a master client index of client information, including a single unique identifier (that is not the Social Security Number), for all clients.	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-18
PG009	4768	1	The solution should maintain an integrated repository of provider agency information, including a single unique identifier, for all providers.	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-18
PG010	3957	1	The solution should be able to capture, verify, and support billing for in-home and community based setting service visits.	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-18
PG011	3959	1	The solution should have the ability to create Health Insurance Portability and Accountability Act (HIPAA)-compliant electronic 837 claim file submission to the State MMIS for claims processing in compliance with all Medicaid filing requirements.	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-18
PG012	4519	1	The solution should automatically generate all required correspondence to individuals.	Program Management	Will Not Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-18
PG013	4523	1	The Vendor should provide correspondence metric reports upon request by the Department.	Program Management	Will Not Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-19
PG014	4552	1	The solution should assist users in identifying which sections of forms should be filled in manually.	Program Management	Will Not Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-19
PG015	4582	1	The solution should provide the ability to deliver reports as mutually agreed-upon with the Department.	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-19
PG016	4381	1	The solution should provide flexible web-based reporting, including ad hoc reporting of all data stored within the solution.	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-20
PG017	4887	1	The solution should have the ability to make a complete set of data related to visits submitted for verifications available for reporting, including, but not limited to the following elements:	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21
PG018	4888	2	Member receiving services	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
PG019	4889	2	Direct care worker	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21
PG020	4890	2	Provider	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21
PG021	4891	2	Location of visit	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21
PG022	4892	2	Date of visit	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21
PG023	4893	2	Start time of visit	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21
PG024	4894	2	Missed visits	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21
PG025	4895	2	Late visits	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21
PG026	4896	2	End time of visit	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21
PG027	4897	2	Visit late time	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21
PG028	4898	2	Services provided	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21
PG029	4900	2	Manual or electronic verification	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21
PG030	4604	1	The solution should have the ability to use identifiers, mathemat	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21
PG031	3992	1	The solution rules/procedures should have the ability to ensure the direct care services do not overlap with other direct care services.	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21
PG032	4209	1	The solution should compile information from all EVV data sources and calculate total daily and weekly hours worked by direct care workers and agencies.	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21
PG033	4211	1	The solution should have the ability for the Department to allow and/or not allow retroactive care plan changes for specific services and/or programs through a configurable interface.	Program Management	Will Not Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21
PG034	4210	1	The solution should allow the Department to define and limit the circumstances in which a manual verification can be made.	Program Management	Will Not Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21
PG035	4184	1	The solution should use eligibility data transferred from the Medicaid Management Information System (MMIS) to determine if any waiver requirements apply. If no waiver requirements apply, the solution should assume that state plan requirements specific to the service being provided apply.	Program Management	Will Not Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-21

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
PG036	4198	1	The Vendor should review the Department waivers and other state plan program requirements to develop and propose system edits that will meet the need of the Department. The Vendor should propose system settings for the Department to consider during the initial solution configuration and during operations. The review and proposal process should happen at an interval defined by the Department.	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-22
PG037	4834	1	The Vendor should provide web portal functionality that addresses the needs of:	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-22
PG038	5013	2	Provider agencies and their direct care workers	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-22
PG039	5224	2	Members	Program Management	Will Not Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-22
PG040	5225	2	Waiver program and/or legal representatives	Program Management	Will Not Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-22
PG041	5014	2	State program staff	Program Management	Will Meet	Attachment 7 – Business Specifications Approach	6.2 Program Management	6-22
PI001	4002	1	The solution should allow the Department the ability to view the same information as a service provider.	Program Integrity	Will Meet	Attachment 7 – Business Specifications Approach	6.3 Program Integrity	6-23
PI002	4214	1	The Vendor should provide a summary of direct care workers and/or provider agencies who demonstrate a high level of missed and late visits, potentially fraudulent services, or potentially fraudulent billing patterns monthly and as requested by the Department.	Program Integrity	Will Meet	Attachment 7 – Business Specifications Approach	6.3 Program Integrity	6-23
PI003	4217	1	The solution should track the time, location, and task performance of direct care workers during service delivery in order to safeguard against fraud, as well as to improve service delivery and program oversight.	Program Integrity	Will Meet	Attachment 7 – Business Specifications Approach	6.3 Program Integrity	6-24
PI004	3991	1	The solution rules/procedures should have the ability to ensure the same direct care worker is not providing services to multiple recipients at the same time at different locations.	Program Integrity	Will Meet	Attachment 7 – Business Specifications Approach	6.3 Program Integrity	6-24
PI005	4084	1	The solution should have the ability to provide role-based reporting to review, analyze, and report all data across categories on a monthly basis and as requested by the Department, including, but not limited to:	Program Integrity	Will Meet	Attachment 7 – Business Specifications Approach	6.3 Program Integrity	6-24
PI006	5208	2	Payers	Program Integrity	Will Meet	Attachment 7 – Business Specifications Approach	6.3 Program Integrity	6-24
PI007	5209	2	Programs	Program Integrity	Will Meet	Attachment 7 – Business Specifications Approach	6.3 Program Integrity	6-24
PI008	5210	2	Provider Agency	Program Integrity	Will Meet	Attachment 7 – Business Specifications Approach	6.3 Program Integrity	6-24
PI009	5211	2	Direct care workers	Program Integrity	Will Meet	Attachment 7 – Business Specifications Approach	6.3 Program Integrity	6-24
PI010	5212	2	Members	Program Integrity	Will Meet	Attachment 7 – Business Specifications Approach	6.3 Program Integrity	6-24

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
PI011	4218	1	The solution should track and report modifications to the solution data input elements after the direct care worker has documented their time or services, including the name of the user making the changes and the reason for the changes.	Program Integrity	Will Meet	Attachment 7 – Business Specifications Approach	6.3 Program Integrity	6-26
VV001	4180	1	The solution should have the ability to verify the delivery of electronic visit verification (EVV) services for multiple programs with different rules and edits.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-6
VV002	4087	1	The solution should have the ability to make a complete set of visit-related data elements submitted for verification available for monthly reporting and as requested by the Department, including, but not limited to:	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-6
VV003	5075	2	Individual receiving services	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-6
VV004	5076	2	Direct care worker	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-6
VV005	5077	2	Billing provider agency	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-6
VV006	5079	2	Location of visit	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-6
VV007	5080	2	Date of visit	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-6
VV008	5081	2	Visit start time	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-6
VV009	5082	2	Visit finish time	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-6
VV010	5083	2	Missed visits	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-6
VV011	5084	2	Late visits	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-6
VV012	5085	2	Services delivered, including billing code and modifiers	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-6
VV013	5086	2	Independent verification by individual receiving services	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-6
VV014	5087	2	Payer	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-6
VV015	5088	2	Manual or electronic verification	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-6
VV016	5089	2	Data collection system, including the Department solution and other approved third party electronic visit verification (EVV) systems	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-6
VV017	4220	1	The solution should have the ability to integrate the scheduling, authorization monitoring, visit verification, and billing.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-7

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
VV018	4183	1	The solution should verify visit components are within program requirements when a visit verification service is initiated and ignore, warn, or stop the user from entering data into the solution as determined by Department.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-12
VV019	4182	1	The solution should securely capture an independent verification of the service delivery from the member receiving services.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-12
VV020	4190	1	The solution should have the ability to allow a direct care worker and/or provider agency to record visits to multiple members within a 24 hour period.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-12
VV021	4191	1	The solution should account for living arrangements in which multiple members receiving services reside at a single address.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-12
VV022	4189	1	The solution should have the ability to allow multiple direct care workers and/or provider agencies to record visits to a member within a 24 hour period.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-13
VV023	4193	1	The solution should have the ability to account for situations in which services are provided to a group of members during a single visit.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-13
VV024	4194	1	The solution should have the ability to account for situations in which the member and the direct care worker reside at the same address.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-13
VV025	4196	1	The solution should account for situations in which a visit starts and/or ends away from the member's place of residence.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-14
VV026	4197	1	The solution should be configurable to either allow or prevent multiple direct care workers and/or provider agencies from providing services to a member at the same time.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-14
VV027	4185	1	The solution should verify that the agency providing the service has a valid pre-authorization for each member served on file.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-14
VV028	4186	1	The solution should verify that the time of the visit is within the parameters outlined on the prior authorization and recorded in a format that can be sorted. The format should be YYYY-MM-DDTHH:MM:SS or equivalent.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-14
VV029	4202	1	The solution should have the ability to allow the Department to identify circumstances in which visit verification is not necessary.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-14
VV030	4203	1	The solution should send real-time alerts when a visit documented in the prior authorization system is not initiated at the scheduled time.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-14
VV031	4195	1	The solution should have the ability to account for circumstances in which a visit crosses calendar days.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-15

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
VV032	4205	1	The solution should accommodate different definitions of pending, late, and missed visits by the status types as defined by the applicable program and/or waiver service.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-15
VV033	4213	1	The solution should allow a direct care worker and/or provider agency to receive messages indicating a possible problem with a visit verification.	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	6.1 Visit Verification	6-16
DD001	5115	1	The Vendor should develop and provide to the Department a Logical Data Model (LDM) that includes, but is not limited to:	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-4
DD002	5116	2	Data classes	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-4
DD003	5117	2	Attributes	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-4
DD004	5118	2	Relationships	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-4
DD005	5119	2	Standards	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-4
DD006	5121	2	Other data elements identified by the Department	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-4
DD007	4088	1	The Vendor should provide a complete list of data elements along with corresponding definitions for reporting purposes, upon request.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-5
DD008	4219	1	The solution should provide real-time access to data entered into the system to provide insight for the services being provided and oversee user activity.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-5
DD009	4497	1	The solution should employ online real-time or batch updates of data between the solution and other systems including, but are not limited to, the Medicaid Management Information System (MMIS) and other third-party Electronic Visit Verification (EVV) systems.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-5
DD010	4513	1	The solution should have the ability to integrate client data for all programs served by the solution into the Master Data Management (MDM) platform.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-6
DD011	4585	1	The solution should allow users to extract data, manipulate the extracted data, and specify the desired format of the output.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-6
DD012	4769	1	The solution should provide required Federal and Department data sharing including high-speed data transfer functionality to send and receive information.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-6
DD013	3997	1	The solutions rules/procedures should allow for electronic communication between the Department, fiscal/employer agents, and providers.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-6

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
DD014	5138	1	The solution should have the ability to store member communications.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-6
DD015	4188	1	The solution should exchange information through interfaces including, but not limited to the Medicaid Management Information System (MMIS), other Electronic Visit Verification (EVV) systems, and others as agreed upon by the Department.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-7
DD016	4398	1	The solution should have the ability to interface with West Virginia's Enterprise Service Bus (ESB).	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-7
DD017	3966	1	The Vendor should complete, subject to approval by the Department, the interface with the Medicaid Management Information System (MMIS).	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-7
DD018	3967	1	The solution should be able to receive information in batch and in individual transactions on a schedule agreed upon by the Department.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-8
DD019	3964	1	The solution should have the ability to receive provider, member, and prior authorization data from the Medicaid Management Information System (MMIS) at a frequency and format determined by the Department.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-8
DD020	3951	1	The solution's data aggregation component should be able to receive a response transaction in a format that is used by the Medicaid Management Information System (MMIS) for the purpose of verifying edits to claims.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-8
DD021	4068	1	The solution should have the ability to apply pre-edit information and serve as a data source for purposes of applying edits during claims processing. The disposition of the edit including, but not limited to deny or suspend, should be determined by the Medicaid Management Information System (MMIS).	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-9
DD022	3952	1	The solution should accept individual and/or batch visit verification inquiries from the Medicaid Management Information System (MMIS).	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-9
DD023	4912	2	Member name	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-9
DD024	4913	2	Billing provider	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-9
DD025	4914	2	Name	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-9
DD026	4915	2	Date	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-9

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
DD027	4916	2	Time of service delivery	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-9
DD028	3954	1	The solution should have the ability to provide visit information to the Medicaid Management Information System (MMIS) by individual and/or in batch format at the discretion of the Department.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-9
DD029	5150	1	The solution should support obtaining member eligibility information through the current Medicaid Management Information System (MMIS) solution using industry standard data interfaces and exchanges as defined by X12N 270/271 transactions (Reference: http://www.wpc-edi.com/)	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-9
DD030	5153	1	The solution should conform to ASC X12 Technical Reports Type 3 (TR3), Version 005010. (Reference: http://www.wpc-edi.com/)	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-10
DD031	4475	1	The solution should generate all forms and notices as necessary.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-10
DD032	4206	1	The solution should have the ability to schedule alerts and user notifications.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-10
DD033	4470	1	The solution should allow printing of blank and completed docur	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-10
DD034	4935	2	All forms	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-10
DD035	4936	2	All system-generated correspondence	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-10
DD036	5104	2	Reports	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-10
DD037	4481	1	The solution should generate and supply forms in the following methods, including, but not limited to:	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-11
DD038	4482	2	Email	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-11
DD039	4483	2	Download from Portal	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-11
DD040	4484	2	Postal Mail, upon request by the Department	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-11

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
DD041	4480	1	The solution should allow the ability to modify field attributes on a form as identified by the Department via the Change Management Plan.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-11
DD042	4478	1	The solution should allow updates to form templates as directed by the Change Management Plan.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-11
DD043	4479	1	The solution should group related correspondence to ensure materials are delivered in a single mailing or posted to a portal account.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-11
DD044	4476	1	The solution should generate the data file containing forms and notices for delivery to the printing vendor for monthly distribution and as requested by the Department.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-11
DD045	4487	1	The solution should automatically populate information on notices or forms being issued.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-11
DD046	4490	1	The solution should generate batch forms.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-11
DD047	4493	1	The solution should save delivered forms to the user's account.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-11
DD048	4521	1	The solution should deliver data files containing all correspondence to the designated printing entity within 24 hours of the correspondence becoming final according to the Department's business rules.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-11
DD049	4527	1	The solution should post finalized correspondence to the web portal, according to the Department's business rules.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-12
DD050	4535	1	The solution should have the ability to produce all correspondence in a printer-friendly 8.5" x 11" format in landscape or portrait orientation.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-12
DD051	4537	1	The solution should have the ability to automatically save a Portable Document Format (PDF) copy of each final correspondence.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-12
DD052	4540	1	The solution should allow users to choose their preferred method of correspondence including, but not limited to, email, post mail, text, or phone.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-12
DD053	4544	1	The solution should generate correspondences using pre-defined templates.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-12
DD054	4546	1	The solution should include automatic system-generated correspondence with output capabilities including, but not limited to:	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-12
DD055	4960	2	Email	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-12

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
DD056	4962	2	Post to user portal account	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-12
DD057	4963	2	Queue for printing	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-12
DD058	4547	1	The solution should be able to schedule distribution of correspondence.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-12
DD059	4561	1	The solution should provide flexible web-based reporting that meets external reporting needs and requirements defined by the Department.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-12
DD060	4085	1	The solution should include a standard library of reports that can be generated by any user with appropriate access.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-13
DD061	4570	1	The solution should have the ability to display the number of pages that should be printed before the user proceeds with printing a report.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-14
DD062	4574	1	The solution should have the ability to export reports directly from the solution into the user-specified format including, but not limited to:	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-14
DD063	4973	2	Excel	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-14
DD064	4974	2	Word	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-14
DD065	4975	2	Hyper Text Markup Language (HTML)	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-14
DD066	4982	2	Comma-Separated Value (CSV)	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-14
DD067	4984	2	Portable Document Format (PDF)	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-14
DD068	4702	1	The solution should provide reporting functionality capable of drilling down from summarized data to detailed data as agreed upon by the Department.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-14
DD069	4879	1	The solution should have an integrated web portal designed to interface, receive, send, and download specified content and reporting information directly from/to entities such as provider agencies, EVV Vendors, contractors, and other state and Federal agencies as part of a fully integrated solution.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-16
DD070	4815	1	The solution should contain the following features and capabilities including, but not limited to:	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-17

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
DD071	4816	2	Drill down and look up functionality to minimize re-entry of information across multiple screens	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-17
DD072	4817	2	Multi-tasking and multiple window capability, including split screens	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-17
DD073	4644	1	The solution should provide context-sensitive help to users on all screens.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-18
DD074	4818	1	The solution should provide menus that are understandable by non-technical users and provide secure access to all functional areas.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-18
DD075	4859	1	The solution should provide a user interface that allows users to move easily throughout the system.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-18
DD076	4839	1	The solution should have the ability to provide public information without requiring authentication for the web portal.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-19
DD077	4862	1	The solution should provide user interface features and capabilities including, but not limited to:	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-19
DD078	4863	2	Pull-down menus and window tabs	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-19
DD079	4864	2	Scalable, true-type screen and printing fonts	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-19
DD080	4865	2	Uppercase and lowercase alphabetic characters	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-19
DD081	4866	2	Ability to tab and mouse-click through data fields and screens	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-19
DD082	4868	2	Consistent theme throughout the site and standardize all headings and footers with index tabs as identified by the Department	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-19
DD083	4875	2	Generated messages that are clear and sufficiently descriptive to provide enough information for problem correction and be written in full English text	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-19
DD084	4884	1	The solution should provide the capability to display confirmation messages for response and request transactions when interfacing with other systems.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-19
DD085	4883	1	The solution should have the ability to allow users to download or print a copy of completed submitted forms.	Data Sources, Delivery, & Display	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-20
DD086	4347	1	The solution should have the ability to perform the following functions including, but not limited to:	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-20

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
DD087	4918	2	Create flags	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-20
DD088	4919	2	Send alerts	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-20
DD089	4920	2	Integration of alerts into the workflow	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-20
DD090	4921	2	Seamlessly integrate the generation of alerts in the workflow management process to a system user-defined group or individual	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach	7.1 Data Sources, Delivery, & Display	7-20
DQ001	3993	1	The solution should provide a method to identify the following:	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-21
DQ002	5049	2	National Provider Identifier (NPI)	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-21
DQ003	5050	2	Healthcare Common Procedure Coding System (HCPCS)	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-21
DQ004	5051	2	International Statistical Classification of Diseases and Related Health Problems, 10th revision (ICD-10) and related modifiers	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-21
DQ005	5136	2	State-specific codes defined by the Department	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-21
DQ006	3965	1	The Vendor should collaborate with the Department to determine how data should be transferred to and from the Medicaid Management Information System (MMIS), including, but not limited to:	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-21
DQ007	5039	2	Definition of data elements	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-21
DQ008	5040	2	Data file formatting	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-21
DQ009	5041	2	Data exchange frequency	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-21
DQ010	5042	2	Thresholds for data quality and acceptance	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-21
DQ011	3953	1	The solution should allow the Department to review and approve data elements included in request and response data exchanges prior to Vendor development or configuration of the solution.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-22
DQ012	3985	1	The Vendor should develop, publish, and maintain a system interface standard for external electronic visit verification (EVV) data partners approved by the Department.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-22
DQ013	4771	1	The Vendor should ensure that file standardization is supported for data element lengths, field format, and type.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-22
DQ014	4781	1	The solution should incorporate a method to view interface files for investigation and further processing.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-22

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
DQ015	4784	1	The solution should create and retain an audit trail of all interface activity in accordance with the Department's Data Retention Policy. (Reference: https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2019/PO1013_DataBackup_Mar2019.pdf	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-22
DQ016	4498	1	The solution should make information about data exchange errors and discrepancies available to the Department and appropriate users monthly.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-22
DQ017	4511	1	The Vendor should provide searchable data schemas and data dictionaries for the solution.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-23
DQ018	4569	1	The solution should report on both duplicated and unduplicated record counts.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-23
DQ019	4588	1	The solution should use consistent data schemes and version control.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-23
DQ020	4765	1	The solution should have the ability to assure data changes made in one part of the solution automatically populate other parts of the system so as to avoid duplicate data entry.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-23
DQ021	4571	1	The Vendor should maintain a comprehensive list of all reports, their intended use, and business area supported.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-23
DQ022	4581	1	The solution should generate a listing of all standard online reports available, the description of each report, and a link to the most recent report for role-based report access.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-23
DQ023	4587	1	The solution should identify and use consistent report fields.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-24
DQ024	4586	1	The solution should display a consistent format on all reports.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-24
DQ025	4597	1	The solution should have the ability to categorize and organize reports including, but not limited to, the following parameters:	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-25
DQ026	4990	2	Source system	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-25
DQ027	4991	2	Data content	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-25
DQ028	4992	2	Purpose	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-25
DQ029	4993	2	Frequency	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-25
DQ030	4774	1	The solution should generate exception reports prior to being submitted to the receiving entity such as the Medicaid Management Information System (MMIS) or other systems receiving electronic visit verification (EVV) data to facilitate data correction by the submitting entity including, but not limited to the following:	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-25

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
DQ031	5095	2	Manual edits	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-25
DQ032	5096	2	Error corrections	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-25
DQ033	5097	2	Additions to the interface records	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-25
DQ034	4778	1	The solution should generate error reports at the summary and detail levels that include all data necessary to resolve errors monthly and as requested by the Department.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-26
DQ035	4584	1	The solution should store reports to allow users the ability to retrieve them quickly per the Department's business rules.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-26
DQ036	4779	1	The solution should reload or resend records if they have not been applied correctly to the receiving entity.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-26
DQ037	4780	1	The solution should detect duplicate files or records and isolate them for manual review and further processing.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-26
DQ038	4782	1	The solution should create messages that accurately describe errors received as a result of a data transfer.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-26
DQ039	4477	1	The solution should have the ability to maintain an up-to-date inventory of all forms utilized and make this inventory available to the Department upon request.	Data Quality	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-26
DQ040	4492	1	The solution should have the ability to identify which fields in forms are required and which are optional.	Data Quality	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-27
DQ041	4530	1	The solution should have the ability to store the date that a correspondence was delivered for printing in a preferred date format of MM/DD/YYYY.	Data Quality	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-27
DQ042	4545	1	The solution should provide automatic default file naming convention for saved correspondence as agreed upon with the Department.	Data Quality	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-27
DQ043	4553	1	The solution should categorize and classify types of correspondence as agreed upon with the Department.	Data Quality	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-27
DQ044	4710	1	The solution should distinguish between, and incorporate, business days, weekends, and state holidays in all time-related functions in the system.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-27
DQ045	4176	1	The solution should include web-based online help functionality in searchable portable document format (PDF), that includes a searchable database of common problems.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-27
DQ046	4472	1	The solution should set parameters on fields to prevent system users from entering information outside of those parameters.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-27
DQ047	4474	1	The Vendor should produce all member- and provider-facing content written at no greater than an eighth grade reading level.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-27

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
DQ048	4880	1	The solution should include email addresses in the authorization table for registration, and email addresses should be kept confidential and only used for official Department business.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach	7.2 Data Quality	7-27
IN001	4759	1	The solution should have the ability to support various current technologies for data interchange and electronic visit verification (EVV) data submission and verification including, but not limited to, web portal, application interface, telephony, quick response (QR) codes, and automated location verification.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-28
IN002	4763	1	The Vendor should utilize open architecture standards and scalability to promote integration throughout the West Virginia technology enterprise.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-29
IN003	4758	1	The solution should be flexible and readily adaptable to changing Department and federal requirements and as requested by the Department.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-29
IN003A	5297	1	The solution should address the disruption or limited availability of network connectivity, telephony, and/or cell coverage at the visit site by providing members and providers more than one method to send and receive electronic visit verification (EVV) data.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-29
IN003B	5298	1	The solution should have the ability to capture and retain electronic visit verification (EVV) data gathered when the transmission services are offline for any reason at the visit site and to send or receive queued system data when services are restored.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-29
IN004	4725	1	The solution should provide archival and purge processes that do not degrade performance or interrupt the system.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-29
IN005	4748	1	The solution should allow centralized deployment of system updates and system maintenance.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-29
IN006	4668	1	The solution should provide workflow functionality that supports a variety of mechanisms to initiate, execute, suspend, or terminate workflows including, but not limited to:	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-30
IN007	5090	2	Communication events (email, document upload, form submissions, or phone)	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-30
IN008	5091	2	System-generated events	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-30
IN009	5092	2	User-triggered events	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-30
IN010	5093	2	Exception-processing events	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-30
IN011	4673	1	The solution should include definition and modeling of workflow processes and their constituent activities.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-30
IN012	4529	1	The solution should have the ability to facilitate mass email notifications.	Hardware and Infrastructure	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-30

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
IN013	4533	1	The solution should have the ability to reissue and track any correspondence or form as requested by the Department.	Hardware and Infrastructure	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-30
IN014	4565	1	The solution should have the ability to schedule any report to be run at varying levels of frequency or on-demand.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-30
IN015	4576	1	The solution should provide integrated print capability within the application for any report.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-30
IN016	4000	1	The solution should have the ability to notify users of system maintenance and other information approved to be distributed by the Department.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-31
IN017	4400	1	The Vendor should manage, track, and report on user support services via multiple channels, including:	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-31
IN018	4401	2	Telephone	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-31
IN019	4402	2	Member portal	Hardware and Infrastructure	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-31
IN020	4403	2	Email	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-31
IN021	4404	2	Mail	Hardware and Infrastructure	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-31
IN022	5215	1	The Vendor should provide investigative results inclusive of mitigation measures to address reported incidents within 30 days of the documented incident.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-31
IN023	4177	1	The Vendor should support provider compliance through direct assistance, coaching, technical assistance, and other active outreach activities as requested by the Department	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-31
IN024	3998	1	The solution should provide users a description of the minimum hardware and software requirements, installation, maintenance, and enhancement of software based on role and system requirements prior to system updates.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-31
IN025	4499	1	The solution should allow users to schedule and modify system events as requested by the Department.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-31
IN026	4408	1	The Vendor should provide a technical support call center located within the contiguous United States.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-32
IN027	4450	1	The solution should document call information, as agreed upon by the Department.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-32
IN028	4410	1	The technical support call center hours of operation should be Monday through Friday, from 9:00 a.m. to 6:00 p.m. Eastern Time (ET) and on an emergency basis as requested by the Department. The call center may be closed for standard federal holidays and West Virginia State holidays,	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-32

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
IN029	4412	1	The Vendor should return all after-hour calls by the next business day, in the caller's preferred language and/or through oral interpretation services. (Reference: https://www.hhs.gov/civil-rights/for-individuals/section-1557/translated-resources/index.html	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-33
IN030	4415	1	The Vendor should provide functionality to manage calls to the Technical Call Center including, but not limited to:	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-33
IN031	4922	2	Creation of tickets	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-33
IN032	4923	2	Editing existing tickets	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-33
IN033	4924	2	Sorting of call center ticket information	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-33
IN034	4925	2	Filtering of call center tickets or electronic records	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-33
IN035	4416	1	The Vendor's Technical Call Center should have the ability to track data including, but not limited to:	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-34
IN036	4417	2	The caller	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-34
IN037	4418	2	The question(s) and/or issue(s)	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-34
IN038	4419	2	The Vendor staff responding to the ticket	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-34
IN039	4420	2	The date(s)	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-34
IN040	4421	2	The time(s)	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-34
IN041	4422	2	The status (opened or closed)	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-34
IN042	5217	2	Problem resolution	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-34
IN043	4431	1	The Vendor's Technical Call Center should have the ability to repeat call options automatically.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-34
IN044	4437	1	The Vendor should maintain sufficient staff and telephone lines to perform all required technical support call center functions.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-34
IN045	4798	1	The solution should use automated menus, including an easily accessible option for reaching a live operator.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-34
IN046	4901	1	The solution should provide assistance to inquiries received from persons who require special assistance including, but not limited to:	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-34
IN047	5031	2	Persons with Limited English Proficiency (LEP)	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-34
IN048	5032	2	Persons with vision disabilities	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-34
IN049	5033	2	Persons with hearing disabilities	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-34

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
IN050	5034	2	Persons with speech disabilities	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-34
IN051	4885	1	The solution should include an online option for users to report any technical problems.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-35
IN052	5190	1	The Vendor should ensure the solution components that are web based have cross-browser compatibility over the life of the contract and support software utilization in the current version and two (2) prior versions at a minimum for the following browsers including, but not limited to:	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-35
IN053	5191	2	Microsoft Edge	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-35
IN054	5192	2	Apple Safari	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-35
IN055	5193	2	Google Chrome	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-35
IN056	5194	2	Mozilla Firefox	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-35
IN057	5195	2	Microsoft Internet Explorer	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-35
IN058	4819	1	The solution should incorporate a non-restrictive environment for experienced users to directly access a screen or to move from one screen to another without reverting to the menu structure.	Hardware and Infrastructure	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-35
IN059	4820	1	The solution should generate drop-down lists to identify options available, valid values, and code descriptions by screen field.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-35
IN060	4835	1	The Vendor should provide web applications that satisfy the Priority 1 Checkpoints from the Web Content Accessibility Guidelines 1.0 developed by the World Wide Web Consortium (W3C), as detailed at: http://www.w3.org/TR/WCAG10/full-checklist.html.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-35
IN061	4838	1	The solution should have the ability to include secure and public facing tabs for the web portal.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-35
IN062	4845	1	The solution should have the ability to utilize an authentication process to handle multiple layers of security levels as requested by the Department.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-35
IN063	4853	1	The solution should have the ability to provide self-service password resets and mask the display of passwords at the sign-on screen when the user enters the portal.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-36
IN064	4854	1	The solution should have the ability to mask the display of passwords at the sign-on screen when entered by the user.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-36
IN065	4882	1	The Vendor should ensure that web portal field definitions comply with system field definitions.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-36

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
IN066	4833	1	The Vendor should, for the web portal, provide Internet security functionality to include firewalls, intrusion detection, and encrypted network/secure socket layer (SSL).	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-36
IN067	5010	1	The Vendor should provide and maintain a secure data storage solution that includes encryption of data in transit and encryption of data at rest.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach	7.3 Hardware and Infrastructure	7-37
SM001	4230	1	The solution should authenticate all users when establishing a connection to the solution.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-40
SM002	3972	1	The solution should have the ability to automatically generate a unique user identification during the registration process for new users enrolling in the program.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-40
SM003	3975	1	The solution should have the ability to assign a new unique user identifier (ID) for an existing user.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-41
SM004	4772	1	The solution should use a secure file transfer protocol (i.e. SFTP, etc.), secure web interface, or other industry-standard electronic means (such as Gentran, Connect: Direct, or equivalent) or encrypted media to transfer files as approved by the Department.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-41
SM005	4224	1	The solution should warn the user about accessing US Government Federally protected data and allow the user to confirm and proceed with such actions.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-41
SM006	4244	1	The Vendor should provide a secure web-based method to receive requests for authorization to access the solution.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-41
SM007	4246	1	The Vendor should provide Single Sign-On (SSO) capability for authentication and authorization across the solution.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-41
SM008	4254	1	The solution should provide Department-approved multi-factor authentication for Vendor remote access to solution environment or their contractors, if applicable.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-41
SM009	3977	1	The solution should use role-based access for data and system functionality.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-41
SM010	3978	1	The solution should have configurable roles by state plan and waiver program that may be created and modified by the Department through a change request as outlined in the Department approved Change Management Plan.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-42
SM011	3983	1	The solution should have the ability to record specific access by users to confidential personal information (CPI) contained within the solution. The mechanism should record the following data elements and allow a role-based user to search this log for matching criteria to discern what was accessed including, but not limited to:	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-42
SM012	5043	2	User name	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-42
SM013	5044	2	Date of access	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-42

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
SM014	5045	2	Time of access	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-42
SM015	5046	2	Name of Individual (First and Last) whose confidential personal information (CPI) was accessed	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-42
SM016	5047	2	Name of computer system used to access confidential personal information (CPI)	Security Management	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-42
SM017	5048	2	Query/Transaction used	Security Management	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-42
SM018	4082	1	The solution should provide users role-based access to reporting functionality.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-42
SM019	5218	1	The solution should allow correspondence to be viewed based on role based access.	Security Management	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-42
SM020	4664	1	The solution should allow authorized users to remove view or edit access rights to any data fields or data elements within the solution based on user role.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-42
SM021	4229	1	The solution should provide role-based security through various methods, including, but not limited to:	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-43
SM022	5052	2	Unique identifiers (IDs)	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-43
SM023	5053	2	Mandatory password standards and policies for length, character requirements, and updates for all users as defined within National Institute of Standards and Technology (NIST) 800-63-3: Digital Identity Guidelines, or equivalent. https://doi.org/10.6028/NIST.SP.800-63-3	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-43
SM024	5054	2	Profile or group access assignments	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-43
SM025	4235	1	The solution should provide a mechanism to limit access to information based on user roles and program rules.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-43
SM026	4236	1	The solution should provide role-based access to all system components and control access through various methods, including, but not limited to:	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-43
SM027	5055	2	Blocking specific window or screen access	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-43
SM028	5056	2	Blocking specific report views or analytics	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-43
SM029	5057	2	Restrict data elements	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-43
SM030	5058	2	Restrict viewing of specific members	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-43
SM031	5059	2	Limit access to other fields within the system as determined by the Department	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-43
SM032	4237	1	The solution should update all security roles automatically when a change in the master role is made.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-43
SM033	4238	1	The solution should allow user access and role changes to be made in real-time.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-43
SM034	4240	1	The solution should have the ability to restrict concurrent logons.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-43

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
SM035	5167	1	The solution should have the ability to configure the timeout requirements for each system environment and user role.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-43
SM036	4204	1	The solution should have the ability to create multi-level escalating alerts for Department-defined events.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-43
SM037	4207	1	The solution should identify the recipients of alerts by alert type and user role.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-44
SM038	3990	1	The solution should have the ability to allow the Department to define which edits and rules may be overridden within the solution by the direct care worker or provider agency and how the solution will respond with warnings, alerts, or denials of the requested user action.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-44
SM039	4319	1	The solution should utilize a Security Information and Event Management (SIEM) solution that generates alerts for events. Copies will be made available to the Department, including, but not limited to:	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-44
SM040	5060	2	Alert generation for attempts to access unauthorized databases from internal and external systems	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-44
SM041	5061	2	Monitoring and reporting of events on an ongoing basis	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-44
SM042	5156	1	The Vendor should provide a report outlining applicable National Institute of Standards and Technology (NIST) SP 800-53 moderate security control responsibilities (reference: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) noting which security controls are implemented and/or inherited by the Vendor, implemented by the Department, or shared by both parties. This report should be maintained by the Vendor and outline the following information, including, but not limited to:	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-45
SM043	5157	2	Non-compliant and required security and privacy controls	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-45
SM044	5158	2	Applied mitigations	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-45
SM045	5159	2	Plan to correct deficiencies	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-45
SM046	4572	1	The solution should maintain a list of users and owners of each stored report.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-45
SM047	4573	1	The solution should retain and maintain access to reports as specified by the Department's Retention Policy. (Reference: https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2019/PO1013_DataBackup_Mar2019.pdf)	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-45

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
SM048	4568	1	The solution should allow, initially, up to fifteen (15) State users to create ad hoc reports. Additional users should be added at no additional cost to the State.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-45
SM049	4590	1	The solution should track and store detailed information regarding all reporting requests, including, but not limited to:	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-46
SM050	4591	2	Who requested the information	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-46
SM051	4592	2	Date of request	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-46
SM052	4593	2	Time of request	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-46
SM053	4594	2	What data the report included	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-46
SM054	4595	2	Report storage upon completion	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-46
SM055	4757	1	The solution should generate a periodic report of upcoming user account terminations on a schedule approved by the Department.	Security Management	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-46
SM056	4801	1	The solution should maintain a record of all Integrated Eligibility Solution (IES) member information accessed.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-46
SM057	4802	1	The solution should maintain a record, including an audit trail, of all manually entered data queries by user, communications, and report distributions.	Security Management	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-46
SM058	5275	1	The Vendor should supply, on an annual basis, a report of the results of all security, privacy, and risk assessments, including all tools used, and an action plan detailing the approach for remediation of security risk vulnerabilities. Data and testing results, including reports, should be retained for 10 years per CMS guidelines.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-46
SM059	4228	1	The solution should log manual overrides and report on them at timed intervals determined by the Department.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-47
SM060	4249	1	The solution should create a log of access attempts and generate a monthly user lock out report to the Vendor's security management team and to the Department, upon request.	Security Management	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-47
SM061	4281	1	The solution should have the ability to provide authorized requestors a report containing the security profile for an individual or role.	Security Management	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-47
SM062	4300	1	The solution should monitor, detect, and report impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.	Security Management	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-47
SM063	4301	1	The Vendor should conduct annual penetration testing of the solution and provide results to the Department within 30 days of completion.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-48

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
SM064	4303	1	The Vendor should provide all incident reporting to the Department immediately upon discovery per Department guidelines.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-48
SM065	4469	1	The solution should be able to redact information contained in any form, correspondence, or report and save the redacted version as a new file.	Security Management	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-48
SM066	4488	1	The solution should allow users to override and change pre-populated information in forms, when appropriate.	Security Management	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-48
SM067	4524	1	The solution should maintain an inventory and store all system-generated correspondence based on Bureau for Medical Services' (BMS) Retention Policy (Reference: https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2019/PO1013_DataBackup_Mar2019.pdf)	Security Management	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-48
SM068	4722	1	The solution should ensure that data, including hard copy documents, are retained, stored, imaged, archived, and protected from destruction. All data should be available according to Department and federal requirements, and in accordance with the Department's Data Retention Policy (Reference: https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2019/PO1013_DataBackup_Mar2019.pdf)	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-49
SM069	4723	1	The Vendor should ensure that hard copy documents are retained, stored, imaged, archived, and destroyed in accordance with applicable federal requirements and in accordance with the Department's Data Retention Policy (Reference: https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2019/PO1013_DataBackup_Mar2019.pdf)	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-49
SM070	4660	1	The solution should prevent certain decisions and fields from having the ability to be overridden by users.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-49
SM071	4837	1	The Vendor should ensure that information captured via the web portal meets the relevant data management specifications, including, but not limited to, access, inquiry, update, retention, and archival.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-49
SM072	4844	1	The solution should have the ability to display and require the user to accept web-site terms of agreement when entering the web portal.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-49
SM073	4846	1	The solution should have the ability to establish user access to predefined Department levels including, but not limited to:	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-49
SM074	5016	2	Page level	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-49
SM075	5017	2	Field level	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-49

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
SM076	5018	2	Data element level	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-49
SM077	4847	1	The Vendor should provide a public facing website that provides access to a secure portal including, but not limited to:	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-50
SM078	4848	2	Instructions on how to use the secure site	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-50
SM079	4849	2	Site map	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-50
SM080	4850	2	Contact information	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-50
SM081	4851	1	The solution should have the ability to send users their initial auto-generated password via email and require that they change their password upon their next sign-on.	Security Management	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-50
SM082	4856	1	The solution should have the ability to require qualifying information to access system records via the web portal including, but not limited to:	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-50
SM083	5021	2	Provider number	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-50
SM084	5022	2	Prior authorization number	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-50
SM085	5023	2	Medicaid ID number	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-50
SM086	5024	2	Date of service	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-50
SM087	5025	2	Claim number	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-50
SM088	4755	1	The solution should allow a system administrator to reset user passwords.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-50
SM089	4756	1	The solution should allow users to change their passwords on demand.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-50
SM090	4852	1	The solution should have the ability to set and adjust password expiration dates.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-50
SM091	5226	1	The solution should have the ability to warn the user that the Caps Lock is on when entering sign-on passwords.	Security Management	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-50
SM092	4231	1	The Vendor should establish an expiration schedule for system component required passwords to minimize system or user disruption.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-51
SM093	4232	1	The solution should store passwords in encrypted form. The Advanced Encryption Standard (AES) 256-bit standard or equivalent should be used. (Reference: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf)	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-51
SM094	4234	1	The solution should enforce password policies for length, character requirements, and updates for all users as agreed upon by the Department	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-51

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
SM095	4241	1	The solution should allow self-service password resets.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-51
SM096	4243	1	The solution should send system-generated email notifications of password change events and expiration warnings at Department approved intervals.	Security Management	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-51
SM097	4242	1	The Vendor should deactivate all system access for users immediately upon notification of termination, departure, or reassignment.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-51
SM098	4248	1	The solution should have the ability to lock out a user after a pre-determined number of unsuccessful login attempts.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-51
SM099	4251	1	The solution should automatically suspend all users who have not accessed the solution within a specified period of time as requested by the Department.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-51
SM100	5166	1	The solution should have the ability to close accounts that have been suspended more than a predetermined number of days as requested by the Department.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-51
SM101	4252	1	The solution should have the ability to terminate authorized sessions after predetermined time period of inactivity, as requested by the Department, after a warning message is displayed to the user informing them that the session will terminate in an identified period of time.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-51
SM102	4749	1	The solution should provide three types of controls to maintain the integrity, availability, and confidentiality of protected health information (PHI) data contained within the system. These controls should be in place at all appropriate points of processing as follows:	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-52
SM103	4750	2	Preventive Controls: Controls designed to prevent errors and unauthorized events from occurring	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-52
SM104	4751	2	Detective Controls: Controls designed to identify errors and unauthorized transactions that have occurred in the system.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-52
SM105	4752	2	Corrective Controls: Controls designed to ensure that the problems identified by the detective controls are corrected.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-52
SM106	4250	1	Upon login, the solution should inform users of privacy policy, including the logging of users' access attempts to personally identifiable information (PII) and/or protected health information (PHI) and other actions taken within the application that are subject to privacy reporting and disclosure notification, including the legal sanctions imposed for improper disclosure and use to be approved by the Department.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-53
SM107	4295	1	The Vendor should deliver reporting on all unauthorized disclosures of personally identifiable information (PII) and/or protected health information (PHI) immediately upon discovery.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-53

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
SM108	4296	1	The Vendor should perform data mapping to identify confidential data and Protected Health Information (PHI) contained in the system, the flow of that data through the system, and where that data resides.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-53
SM109	4258	1	The Vendor staff should adhere to all Department security requirements when on-site at Department facilities and as required by the facility's security requirements.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-53
SM110	4262	1	The Vendor should protect the Vendor's data center location(s) against intrusion at all times and maintain a surveillance alarm system that is linked to a manned monitoring center.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-53
SM111	4263	1	The Vendor should provide the Department access to all facilities to conduct announced and unannounced visits of the Vendor's facilities.	Security Management	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-53
SM112	4264	1	The Vendor should maintain a current database of individuals who have access to its facilities and the database should be available for the Department's inspection upon request.	Security Management	Will Not Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-54
SM113	3976	1	The solution should have the ability to reassign existing records from one user identifier (ID) to another user ID in the case of fraud, errors, and omissions that affect data integrity and reporting according to the Department's business rules. All reassignment of records should be captured in audit logs.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-54
SM114	4265	1	The solution should audit and track all activity specific to each user including, but not limited to:	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-54
SM115	4266	2	Invalid login attempts	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-54
SM116	4267	2	Transaction activities	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-54
SM117	4268	2	Track adds, changes, and deletes of individual member visit verification data	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-54
SM118	4269	2	Password changes	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-54
SM119	4270	2	Security question and/or Key creation	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-54
SM120	4271	2	Updates to security questions	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-54
SM121	4272	2	User navigation history	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-54

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
SM122	4225	1	The Vendor should ensure that its employees and subcontractors complete and maintain required security training and follow State and Department policies regarding security. This should be done, at a minimum, on an annual basis and for all new hires within five (5) business days of being hired (Reference: https://www.wv.gov/Policies/Pages/default.aspx#undefined)	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-54
SM123	4275	1	The solution should collect sufficient detail to produce an immutable audit log of all manual and automated system activity including, but not limited to the following elements:	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-55
SM124	4276	2	User Identification	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-55
SM125	4277	2	Machine/Internet Protocol Address Identification	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-55
SM126	4278	2	Time and Date of Action	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-55
SM127	4279	2	Actions Performed	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-55
SM128	4282	1	The solution should record an immutable audit log of security role assignment and revocation activities performed within the solution and changes to security role assignments on servers and in databases.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-55
SM129	4257	1	The Vendor should disable building and system access in real-time for staff upon termination, departure, or reassignment from the project.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-55
SM130	4283	1	The solution should generate audit reports based on a request from authorized requestors at the Department.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-55
SM131	5288	1	The solution should have the ability to control access to member records based on user roles and system credentials.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-55
SM132	4247	1	The solution should support member-delegated authority including, but not limited to:	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-56
SM133	5161	2	Assistors	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-56
SM134	5162	2	Authorized representatives	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-56
SM135	5295	1	The Vendor should require that all employees accessing sensitive and critical member data successfully pass State and Federal fingerprint-based background checks prior to potential or actual data access. See request for proposal (RFP) Section 3: General Terms and Conditions for more information.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-56

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
SM136	4315	1	The Vendor should conduct information security assessments and audits of the solution to be conducted by the Vendor, by the Department, or by an external entity hired by the Department as directed by the Department.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-56
SM137	4318	1	The Vendor should conduct all security, privacy, and/or risk assessments inclusive of vulnerability scans of the solution and the results of the vulnerability scan should be included with the assessment results.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-57
SM138	3989	1	The Vendor should allow for only Department approved users to enter and/or approve change request activities, per the Change Management Plan.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-57
SM139	5151	1	The solution should comply with the standards and protocols under sections 1104 and 1561 of the Affordable Care Act (ACA). (Reference: https://www.caqh.org/core/operating-rules-mandate) (Reference: https://www.healthit.gov/sites/default/files/rules-regulation/aca-1561-recommendations-final2.pdf)	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-57
SM140	5154	1	The Vendor should follow Federal, State, and Department policies for receipt and removal of hardware and electronic media that contain electronic protected health information according to 45 CFR164.310. (Reference: HTTPs://www.hhs.gov/sites/default/files/patient-protection.pdf)	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-57
SM141	4754	1	The solution should allow local and central system security administrators to add and change permissions for local and central system access.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-57
SM142	4288	1	The Vendor should maintain the same level of security compliance during any interruption of normal operations as outlined in the RFP Contract Deliverables and applicable federal requirements.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-58
SM143	4289	1	The solution should have the ability to securely access all data in the event of an emergency without any impacts to the confidentiality or integrity of the data.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-58
SM144	4305	1	The Vendor should deliver the system architectural activity and process diagrams that detail security and privacy controls to the Department upon request.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-59
SM145	4307	1	The Vendor should ensure that all Vendor-owned hardware and software are configured securely, including but not limited to:	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-60
SM146	4308	2	Being protected by industry standard virus protection software, which is automatically updated according to a Department-approved schedule.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-60
SM147	4309	2	Having all security patches installed that are relevant to the applicable operating system and all other system software and hardware.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-60

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
SM148	4310	2	Maintaining compatibility with Department software and systems.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-60
SM149	4311	2	Utilizing only licensed software and hardware solutions that have not been classified as End-of-Life (EOL).	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-60
SM150	4312	1	The Vendor should ensure they are in compliance with the State and Department Information Technology Security and Privacy Policies.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-60
SM151	4320	1	The Vendor should maintain documentation of encryption keys, interface credentials, and service account credentials, and provide the Department with updated documentation every time an update is made.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-61
SM152	4321	1	The Vendor should provide continuous monitoring of the solution using intrusion detection software (IDS).	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-61
SM153	4322	1	The Vendor should provide reports at intervals as agreed upon by the Bureau from the intrusion detection software (IDS).	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-61
SM154	4323	1	The Vendor should provide continuous monitoring of the solution using industry standard intrusion prevention software (IPS).	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-61
SM155	4324	1	The Vendor should provide reports at intervals agreed upon by the Department from the intrusion prevention software (IPS).	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-61
SM156	4328	1	The solution should have the ability to support non-disclosure of information.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-61
SM157	4429	1	The Vendor's Technical Call Center should have the ability to authenticate the caller/user as required by the Department.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-61
SM158	4313	1	The solution should provide complete logical and physical segregation of electronic visit verification (EVV) data and files from the data and files of other Vendor/Vendor customers.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach	7.4 Security Management	7-61
PM001	3963	1	The solution should have the ability to modify settings through the approved Change Management Plan to configure the business rules engine performing tasks, including, but not limited to:	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-11
PM002	5036	2	Rule deletion	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-11
PM003	5037	2	Rule modification	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-11
PM004	5038	2	Addition of new rules	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-11
PM005	5146	2	Business edits	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-11

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
PM006	5147	2	Others as defined by the Department	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-11
PM007	3979	1	The Vendor should collaborate with the Department to establish the initial roles and level of access and responsibility for each class of user.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-11
PM008	3982	1	The solution and supporting processes should comply with the Centers for Medicare & Medicaid Services (CMS) Seven Conditions and Standards and the most current version of CMS Medicaid Information Technology Architecture (MITA). (Reference: https://www.medicaid.gov/Medicaid-CHIP-Program-Information/By-Topics/Data-and-Systems/Downloads/EFR-Seven-Conditions-and-Standards.pdf)	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-11
PM009	4130	1	The Vendor should conduct an overview with the Department of solution changes that are ready to be moved into the production environment as directed in the Change Management Plan.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-13
PM010	4711	1	The Vendor should request authorization in writing from the Department prior to promoting any system changes to the production environment or solution as agreed upon by the department.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-13
PM011	4199	1	The solution should have the ability to allow the modification of edits per the Change Management Plan.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-13
PM012	4212	1	The Vendor should provide a manual visit verification process that is adaptable to changes in program requirements throughout the contract period as directed by the Change Management Plan.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-13
PM013	4083	1	The solution reporting should be configurable so that standard reports and recipients of reports can be changed easily over the life of the contract without additional cost, as defined in the approved Change Management Plan.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-14
PM014	4174	1	The Vendor should update the user manual and receive Department approval each time a solution change or upgrade is implemented as directed by the Change Management Plan and within an agreed upon time-frame by the Department.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-14
PM015	4175	1	The Vendor should provide updates to the user manual and have the updated manual available to users no later than thirty (30) days prior to the date a solution change is implemented as directed by the Change Management Plan.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-14
PM016	3999	1	The Vendor should configure the solution for specific Medicaid waivers/services at no additional cost to the Department, per the Change Management Plan.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-14

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
PM017	5113	1	The solution should have the ability to support data integrity through system controls for software program changes and promotion to production as defined in the approved Change Management Plan.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-14
PM018	4676	1	The solution should support workflow development by the vendor based on new processes defined by the Department according to business needs as identified in the Change Management Plan.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-15
PM019	4712	1	The solution should have the ability for the Department to control and monitor system change requests as defined in the approved Change Management Plan.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-15
PM020	4714	1	The solution should have the ability for the Department to set and change priority levels on individual change requests as defined in the approved Change Management Plan.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-15
PM021	4317	1	The Vendor should conduct a security, privacy, and/or risk assessment of any new functionality prior to its deployment to production , the results of which should be delivered to the Department within an agreed upon timeframe by the Department. The Vendor should obtain Department approval for proposed resolutions to all assessment findings prior to deployment to production per the Change Management Plan.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-15
PM022	4116	1	The Vendor should coordinate all testing activities as agreed upon by the Department.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-15
PM023	4117	1	The Vendor should prepare a comprehensive set of test scenarios, within a timeframe as agreed upon by the Department, including but not limited to:	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-16
PM024	5198	2	Applicable test cases	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-16
PM025	5199	2	Expected test results	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-16
PM026	5200	2	Others as defined by the Department	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-16
PM027	4118	1	The Vendor should provide the Department and/or its designees access to test cases and test data to facilitate execution of applicable testing cycles.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-16
PM028	4119	1	The Vendor should provide the Department with a fully tested and operations-ready User Acceptance Test environment that is isolated and separate from all other environments.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-16

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
PM029	4129	1	The Vendor should discuss and finalize with the Department the level of testing required based on the significance of the change as directed in the Change Management Plan.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-16
PM030	4131	1	The Vendor should provide the Department weekly reports of testing status, including, but not limited to.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-16
PM031	5201	2	Metrics on the number of tests completed	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-16
PM032	5202	2	Number of deferred or canceled tests	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-16
PM033	5203	2	Results of the tests executed	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-16
PM034	5204	2	Defects identified by severity level	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-16
PM035	5205	2	Corrective actions taken	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-16
PM036	5206	2	Others as defined by the Department	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-16
PM037	4141	1	The Vendor should conduct Pilot Testing to validate the capacity and processing capabilities of the solution in a tightly controlled production environment.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-16
PM038	4142	1	The Vendor should include a test of actual data processing in a full operational environment, with successful end-to-end solution functionality during Pilot Testing.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-17
PM039	4144	1	The Vendor should provide written test results of the Pilot Testing to the Department within an agreed upon timeframe.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-17
PM040	4145	1	The Vendor should provide the Department official written notification of readiness for full production operations after completion of Pilot Testing.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-17
PM041	3986	1	The Vendor should work with the Department to develop an interface testing acceptance standard to outline the minimum requirements that must be met prior to allowing external electronic visit verification (EVV) data partners to submit data to the EVV solution.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-17
PM042	3987	1	The Vendor should conduct interface testing with external electronic visit verification (EVV) data partners approved by the Department.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-17

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
PM043	4785	1	The Vendor should provide testing and training environments that include sufficient, representative data elements that are in the production environment. The Vendor should not invoke or charge the Department for license fees for any of the testing or training environments.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-17
PM044	4786	1	The Vendor should use a User Acceptance Testing (UAT) environment that mirrors all programs in production to allow the Department to conduct testing prior to new software updates and to serve as an ongoing training platform for users.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-18
PM045	4788	1	The Vendor should create, use, and make available to the Department, representative samples for testing edits, business rules, and workflow processing.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-18
PM046	4789	1	The Vendor should create or modify existing data as needed for testing in a test environment, in compliance with federal guidelines. (Reference: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Downloads/TestingFramework.pdf)	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-18
PM047	4790	1	The Vendor should maintain a clearly organized test case library that can be accessed by all testers, including Department users, with search capability that is cross-referenced to the code that it tests.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-18
PM048	4836	1	The Vendor should ensure web portal design, development, implementation (DDI) and operations are in accordance with Department and federal regulations and guidelines related to security, accessibility, confidentiality, and auditing. (Reference: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/IS_Policy-.pdf)	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-18
PM049	5227	1	The solution should be developed and implemented in accordance with the project work plan.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-18
PM050	5244	1	The Vendor should conduct the following types of testing in support of the solution:	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-19
PM051	5245	2	Unit testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-19
PM052	5247	2	Iterative functional testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-19
PM053	5248	2	System integration testing (SIT)	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-19

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
PM054	5249	2	Interface testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-19
PM055	5250	2	Regression testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-19
PM056	5251	2	End-to-end testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-19
PM057	5252	2	Security testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-19
PM058	5253	2	Performance testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-19
PM059	5254	2	Usability/Accessibility testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-19
PM060	5255	2	Browser testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-19
PM061	5256	2	User acceptance testing (UAT)	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-19
PM062	5257	2	Data conversion testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-19
PM063	5258	2	Operational readiness testing (ORT)	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-19
PM064	5259	2	Other testing as identified by the Department and/or Vendor	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-19
PM065	5260	1	The Vendor should be prepared to assist the Department, as necessary, with User acceptance testing (UAT).	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-21
PM066	5261	1	The Vendor should be prepared to conduct User acceptance testing (UAT) in all cases whereby the Department does not elect to conduct UAT.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-21
PM067	5262	1	The Vendor should complete regression testing subsequent to, but not limited to, the following:	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-22
PM068	5263	2	Deployment of new solution components	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-22
PM069	5264	2	Integration of each solution component into the primary solution	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-22

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
PM070	5265	2	Every migration of new build versions to each test environment	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-22
PM071	5266	2	Solution fixes	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-22
PM072	5267	2	Solution patches	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-22
PM073	5268	2	Solution releases	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-22
PM074	5269	2	Others as defined by the Department	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-22
PM075	5270	1	The Vendor should utilize a subset of system integration testing (SIT) scenarios representative of maximum functional and technical solution coverage for the purposes of regression testing.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-22
PM076	5271	1	The Vendor should obtain approval from the Department on which scenarios should be used for regression testing.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-22
PM077	5272	1	The Vendor should utilize end-to-end test cases in support of regression testing.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-22
PM078	5273	1	The Vendor should perform privacy and security testing on functional, technical, and infrastructure components to ensure the solution meets all State, Department, and Federal privacy and security requirements. (Reference: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/IS_Policy-.pdf)	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-22
PM079	5274	1	The Vendor should propose testing scenarios and/or cases to the Department for their approval.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-23
PM080	5276	1	The Vendor's performance testing methodology should allow for performance tests to be representative of the expected peak period volumes for solution operation.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-23
PM081	5277	1	The Vendor's performance testing should occur on a production ready version of the solution.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-24
PM082	5278	1	The solution's performance testing environment should mirror the final production solution specifications.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-24
PM083	5279	1	The Vendor should perform usability/ accessibility testing for various types of users, including, but not limited to:	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-24

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
PM084	5280	2	Internal users	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-24
PM085	5281	2	External users	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-24
PM086	5283	2	Users with limited computer skills	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-24
PM087	5284	2	New user registration	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-24
PM088	5286	2	Users with disabilities	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-24
PM089	5287	2	Others as defined by the Department	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-24
PM090	4133	1	The Vendor should conduct an Operational Readiness Review (ORR) prior to statewide implementation of the solution.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-24
PM091	4136	1	The Vendor's Operational Readiness Review (ORR) testing should include a volume/stress test of at least 30 calendar days of production-capacity volumes to demonstrate that the solution and Vendor staff members are prepared for full production.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-24
PM092	4138	1	The Vendor should document and propose solutions, and timeframes for corrective actions to all issues, problems, and defects identified through the Operational Readiness Review (ORR).	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-25
PM093	4140	1	The Vendor should prepare and submit to the Department an Operational Readiness Review (ORR) Report that demonstrates that the Vendor and solution are ready to begin operations.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-25
PM094	4566	1	The Vendor should correct any report errors identified by the Department or the Vendor and correct the report within an agreed upon timeframe, through additional steps as defined in the Change Management Plan, including, but not limited to:	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-25
PM095	4969	2	Correct the report	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-25
PM096	4970	2	Verify the report	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-25
PM097	4971	2	Distribute or re-distribute the report	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-25

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
PM098	4972	2	Others actions as defined by the Department	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-25
PM099	4089	1	The Vendor should assist the Department with specialized research and reporting as requested.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-25
PM100	4787	1	The Vendor should be able to test edits, business rules, and workflow processing and report on results.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-25
PM101	5171	1	The Vendor should support either the transition of the solution to an entity designated by the Department and/or support the retirement of the solution at the end of the term of the contract, including all contract extensions as defined in the Turnover and Closeout Management Plan.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-26
PM102	4448	1	The Vendor should obtain Department approval of all scripts prior to implementation that will be used in the Technical Call Center.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-26
PM103	4508	1	The Vendor should identify and be responsible for the implementation and integration of all third-party software used in support of the solution.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-26
PM104	5228	1	The Vendor should conduct requirements validation and joint application design in support of requirements analysis and solution design activities as agreed upon by the Department.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-26
PM105	5229	1	The Vendor should maintain a requirements traceability matrix (RTM) throughout the lifecycle of the project.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-27
PM106	5230	1	The Vendor should provide all stakeholders identified by the Department access to the requirements traceability matrix (RTM).	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-27
PM107	5231	1	The Vendor should document in the requirements traceability matrix (RTM) where each requirement is accounted for, including, but not limited to:	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-27
PM108	5232	2	Design documentation	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-27
PM109	5233	2	Code modules	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-27
PM110	5234	2	Test conditions	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-27
PM111	5235	2	Test scenarios	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-27

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
PM112	5236	2	Test cases	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-27
PM113	5237	2	Certification criteria	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-27
PM114	5238	2	Medicaid Information Technology Architecture (MITA) business areas and processes	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-27
PM115	5239	2	Medicaid Information Technology Architecture (MITA) Standards and Conditions	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-27
PM116	5240	2	Others as defined by the Department	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-27
PM117	5241	1	The Vendor should demonstrate through the requirements traceability matrix (RTM) that all documented and approved specifications have been traced throughout the development lifecycle.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-28
PM118	5242	1	The Vendor should work with the Department during joint application design (JAD) sessions to validate the scope, purpose, and implications of each Request for Proposal (RFP) specification.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-28
PM119	5243	1	The Vendor should identify and work to resolve gaps between the Vendor's and the Department's understanding of a specification(s) during joint application design (JAD) sessions.	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach	8.1 Project Management Methodology	8-28
TN001	3973	1	The Vendor should provide outreach to users to ensure and document their readiness to begin using the solution. The outreach should include all user groups including, but not limited to:	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-42
TN002	5176	2	Members or Legal Representative	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-42
TN003	5177	2	Direct Care Workers	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-42
TN004	5178	2	Provider Agencies	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-42
TN005	5197	2	The Department	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-42
TN006	5179	2	Other as defined by the Department	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-42

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
TN007	3974	1	The Vendor should provide training at the time of registration.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-42
TN008	4146	1	The Vendor should collaborate with the Department and the stakeholder community to develop strategies to train members receiving services.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-44
TN009	4149	1	The Vendor should provide both web-based and ten (10) state-wide in-person trainings to users prior to the initial implementation of the solution based on a schedule and locations as agreed upon by the Department.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-44
TN010	4152	1	The Vendor should provide written training materials for both in-person and web-based training options.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-44
TN011	4153	1	The Vendor should submit all training materials to the Department for review and approval at least 45 calendar days prior to the date of the first training session.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-44
TN012	4154	1	The Vendor should provide training materials offered in accessible formats consistent with requirements of the Americans with Disabilities Act (ADA) throughout the life of the solution. (Reference: https://www.ada.gov/regs2010/titleII_2010/titleII_2010_regulations.pdf)	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-44
TN013	4155	1	The Vendor should provide training materials and training courses that are accessible for users who do not speak, read, or write the English language, upon request by the Department according tohttps://www.hhs.gov/civil-rights/for-individuals/section-1557/translated-resources/index.html.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-45
TN014	4156	1	The Vendor should obtain independent verification of the accuracy of all translations made pursuant to language and accessibility requirements.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-45
TN015	4158	1	The Vendor should provide web-based training available to users throughout the life of the solution.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-45
TN016	4160	1	The Vendor should provide a detailed approach to user training with respect to solution modifications.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-45
TN017	4161	1	The solution should maintain a record of all user training, including the name of the individual trained, the date of training, the specific training completed, and whether the training was in-person or web-based.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-45
TN018	4162	1	The Vendor's training records should be included in the data available for reporting.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-45
TN019	4168	1	The Vendor should provide a user manual to all users.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-46

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
TN020	4169	1	The user manual should be subject to Department approval.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-46
TN021	4170	1	The user manual should be available online and in hard copy upon request of the user.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-46
TN022	4171	1	The user manual should be offered in accessible formats consistent with requirements of the Americans with Disabilities Act. (Reference: https://www.ada.gov/regs2010/titleII_2010/titleII_2010_regulations.pdf)	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-46
TN023	4172	1	The user manual should be available in at least those languages the Department is required to accommodate, in addition to English, pursuant to 45 Code of Regulations (CFR) Section 80.3(b)(2). (Reference: https://www.hhs.gov/civil-rights/for-individuals/section-1557/translated-resources/index.html)	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-46
TN024	5289	1	The solution should support workforce security awareness through such methods including, but not limited to:	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-47
TN025	5290	2	Security reminders (at login or screen access)	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-47
TN026	5291	2	Training reminders	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-47
TN027	5292	2	Online training capabilities	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-47
TN028	5293	2	Training tracking	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-47
TN029	5294	2	Others as defined by the Department.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach	8.4 Training	8-47
DR001	4735	1	The solution should provide sufficient transaction logging and database back-up to allow it to be restored. If multiple databases are used for work item routing and program data, restoring the solution should ensure that databases are synchronized to prevent data corruption.	Solution Back-up, Disaster Recovery, and Failover	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.2 Solution Backup, Disaster Recovery, and Failover	9-13
DR002	4453	1	The solution should have the ability to perform online backups without interruption to production operations, according to a schedule agreed upon by the Department.	Solution Back-up, Disaster Recovery, and Failover	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.2 Solution Backup, Disaster Recovery, and Failover	9-13
DR003	4737	1	The solution should allow continued use of the system during back-up and perform back-ups during non-peak processing hours, to minimize the impact to operational activities.	Solution Back-up, Disaster Recovery, and Failover	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.2 Solution Backup, Disaster Recovery, and Failover	9-13

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
DR004	4331	1	The solution should support data freezing.	Solution Back-up, Disaster Recovery, and Failover	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.2 Solution Backup, Disaster Recovery, and Failover	9-13
DR005	4261	1	The Vendor should maintain an operational back-up power supply capable of supporting vital functions.	Solution Back-up, Disaster Recovery, and Failover	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.2 Solution Backup, Disaster Recovery, and Failover	9-14
DR006	4290	1	The Vendor should equip facilities with proper safeguards for fire prevention, fire detection, and fire suppression that are consistent with local fire codes.	Solution Back-up, Disaster Recovery, and Failover	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.2 Solution Backup, Disaster Recovery, and Failover	9-14
DR007	4291	1	The Vendor should equip fire detection and alarm systems with uninterruptable power supply.	Solution Back-up, Disaster Recovery, and Failover	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.2 Solution Backup, Disaster Recovery, and Failover	9-14
DR008	4293	1	The Vendor should have a remote backup facility at least one hundred (100) miles away from the primary data center.	Solution Back-up, Disaster Recovery, and Failover	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.2 Solution Backup, Disaster Recovery, and Failover	9-14
DR009	4292	1	The Vendor should conduct an annual disaster recovery exercise at a mutually agreed upon time and provide the results to the designated Department staff. Department staff should be invited to be included in these exercises.	Solution Back-up, Disaster Recovery, and Failover	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.2 Solution Backup, Disaster Recovery, and Failover	9-14
DR010	5114	1	The Vendor should store all backup copies in a Department-approved backup storage location for a period of time specified by the Department.	Solution Back-up, Disaster Recovery, and Failover	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.2 Solution Backup, Disaster Recovery, and Failover	9-14
OP001	4715	1	The Vendor should track, and provide the Department access to, process metrics and other detail as defined in the approved Change Management Plan, including, but not limited to:	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-3
OP002	4716	2	The estimated and actual hours allocated to each change request	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-3
OP003	4717	2	Specific personnel assigned to each change request	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-3
OP004	4718	2	Scheduled completion date for each change request	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-3
OP005	4719	2	Total cost if the maximum allowed hours are exceeded on any approved change request	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-3

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
OP006	4720	2	Any change to current operational costs	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-3
OP007	4721	2	A separate total for equipment requirements (if applicable) related to the modification	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-3
OP008	5008	2	Others as defined by the Department	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-3
OP009	4743	1	The Vendor should assure all production software updates, releases, and patches are evaluated and approved by the Department prior to implementation as defined in the Change Management Plan.	Operations	Will Not Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-3
OP010	4744	1	The Vendor should send notification to the Department when releases are available to be evaluated as defined in the Change Management Plan.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-3
OP011	4745	1	The Vendor should provide the Department with detailed documentation that provides all fixes and functionality for each release.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-3
OP012	4747	1	The Vendor should maintain version control and provide the Department with current system and user documentation.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-3
OP013	3988	1	The Vendor should perform all maintenance and product upgrades for all operational and test environments and hardware at no additional cost so that the system is operating on currently supported version of each product and maintain software and security patches, based on a schedule approved by the Department.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-4
OP014	3960	1	The solution should provide the ability for the provider agency to review billing prior to submitting for payment.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-4
OP015	5130	1	The solution should provide the ability for the provider agency to review and correct billing errors prior to submission.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-4
OP016	3961	1	The solution should provide the Department and provider agencies with reports of unbilled encounters through front-end edits including, but not limited to:	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-5

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
OP017	5131	2	No authorization	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-5
OP018	5132	2	Expired authorization	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-5
OP019	5133	2	Reasons that prevented claims from filing	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-5
OP020	5134	2	Edits made to claims	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-5
OP021	5135	2	Others as defined by the Department	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-5
OP022	3955	1	The Vendor should provide a report of all daily transactions, including interactions via the call center, available to the Department in a variety of formats, including, but not limited to:	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-5
OP023	5100	2	Browser-based	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-5
OP024	5101	2	Portable Document Format (PDF)	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-5
OP025	5102	2	Excel	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-5
OP026	5103	2	Comma-Separated Value (CSV)	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-5
OP027	5172	2	Others as defined by the Department	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-5
OP028	4522	1	The solution should track metrics for each type of correspondence generated in the solution.	Operations	Will Not Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-5

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
OP029	4526	1	The solution should track the status of notices that are moving through the generation process.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-5
OP030	4528	1	The solution should notify the Department when an undelivered scheduled system-generated correspondence is approaching the predetermined delivery timeframe as agreed upon by the Department.	Operations	Will Not Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-5
OP031	4534	1	The solution should have the ability to track when any correspondence or form has been reissued or revised as agreed upon by the Department.	Operations	Will Not Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-5
OP032	4902	1	The Vendor should pay and arrange for an annual Statement on Standards for Attestation Engagements, System, and Organization Controls (SOC) 1, Type II audit, using the most current version of the audit, which should cover work performed by the Vendor at the Vendor's facility and data center sites. (Reference: https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2019/PO1008_Audit_Mar2019.pdf)	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-6
OP033	4903	1	The Vendor should submit the annual Statement on Standards for Attestation Engagements, System, and Organization Controls (SOC) 1, Type II audit report, using the most current version of the audit, to the Department for approval with an action plan to remediate findings within a timeframe agreed upon by the Vendor and the Department.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-6
OP034	4253	1	The solution should archive and store user profiles for a period of time agreed upon by the Department.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-6
OP035	5214	1	The Vendor should provide its incident reporting procedures to the Department for review and approval within a timeframe agreed upon by the Department.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-6
OP036	4164	1	The Vendor should detail the performance metrics and targets used to monitor the effectiveness of technical support by phone.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-6
OP037	4165	1	The solution should have the ability to provide an immediate response acknowledging all email inquiries and establishing a timeframe for the response.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-6
OP038	4166	1	The solution should have the ability to resolve all email inquiries to the Vendor's technical support within one 24 hour business day from initial receipt.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-6

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
OP039	4167	1	The Vendor should document inquiries and provide the Department with routine reports regarding reasons for technical support requests.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-6
OP040	4178	1	The Vendor should document any procedural action that occurred as a result of a complaint to the helpdesk and submit this documentation to the Department on an agreed upon schedule.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-7
OP041	4447	1	The Vendor's Technical Call Center should provide a toll-free voice messaging system that is compliant with the Americans with Disabilities Act (ADA) and supports limited English proficiency as defined by the Department of Health and Human Services (HHS). (References: https://www.ada.gov/regs2010/titleII_2010/titleII_2010_regulations.pdf, https://www.hhs.gov/civil-rights/for-individuals/special-topics/limited-english-proficiency/index.html). The Technical Call Center should function 24 hours per day, 365 days per year, and provides callers information including, but not limited to:	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-8
OP042	4928	2	Hours of operation	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-8
OP043	4929	2	Options for leaving messages after hours	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-8
OP044	4930	2	Options for leaving messages based on queue hold times and designated intervals as defined by the Department	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-8
OP045	4931	2	Recording of informational messages as defined by the Department	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-8
OP046	5107	1	The solution should have the ability to record and report on the performance and utilization of resources within the overall system, including, but not limited to:	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-8
OP047	5108	2	Average speed of answer	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-8

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
OP048	5109	2	Interface processing time	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-8
OP049	5110	2	Request time for report generation	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-8
OP050	5111	2	Others as defined by the Department	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-8
OP051	4500	1	The Vendor should document and maintain technical specifications associated with the solution including, but not limited to:	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-9
OP052	4501	2	Complete listing of all software, hardware, and configurations that are required to establish fully functional installations in each of the required environments.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-9
OP053	4502	2	Complete specifications for all software, environments, and hardware used to support the solution.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-9
OP054	4939	2	Others as defined by the Department	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-9
OP055	4504	1	The Vendor should provide the Department with a capacity analysis report for the solution and the hosted environment including, but not limited to:	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-9
OP056	4940	2	Hardware	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-9
OP057	4941	2	Environment	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-9
OP058	4942	2	Network specifications	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-9
OP059	5106	2	Others as defined by the Department	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-9

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
OP060	4661	1	The solution should provide real-time solution performance data.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-9
OP061	4663	1	The solution should report on total processing times based on user-defined queries.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-10
OP062	4739	1	The solution should write all errors to an error log in a standard format and make it available for Department review upon request.	Operations	Will Not Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-10
OP063	4740	1	The solution should allow the Department's administrator to view, filter, sort, and search the error log(s).	Operations	Will Not Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-10
OP064	4746	1	The Vendor should notify the Department regarding which releases of third-party software (JAVA virtual machine, Internet Explorer, Mozilla, Safari, etc.) are known to create problems with the current version of the Vendor software.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-10
OP065	4773	1	The solution should schedule and support file transfers as requested and agreed upon by the Department.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-10
OP066	3946	1	The solution's data aggregation component should send each provider agency a verified visit report, at least once a calendar day.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-11
OP067	3948	1	The solution's data aggregation component should send each provider agency a visit not verified report showing visits that were not verified by the provider agency, at least once each calendar day.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach	9.1 Operations	9-11