Request For Proposal Response

West Virginia Department of Health and Human Resources Bureau of Medical Services

CRFP 0511 BMS2000000001

RECEIVED
2020 MAR 12 AM 8:14
WV PURCHASING DIVISION

TELLUS

TABLE OF CONTENTS

Certification and Signature Page 02
Executive Summary 04

Attachment 3: Vendor Qualifications and Experience 09
Attachment 4: Project Organization and Staffing Approach 25
Attachment 5: Initial Work Plan 50
Attachment 6: Mandatory Requirements 60
Attachment 7: Business Specifications Approach 81
Attachment 8: Technical Specifications Approach 115
Attachment 9: Implementation Specifications Approach 212
Attachment 10: Maintenance and Operations Specifications Approach 288

Addendums 305
Addendum A: West Virginia Draft Project Schedule
Addendum B: West Virginia Draft Work Breakdown Structure
Addendum C: Payer Integration Test Plan
Addendum D: Change Management
Addendum E: Risk Management
Addendum F: Transition or Termination policy
Addendum G: Disclosure of Interested Parties
Addendum H: EVV Appendix 1 - Detailed Specifications
Addendum I: EVV Appendix 6 - Mandatory Requirements
Addendum J: Purchasing Affidavit
Addendum K: Addendum Acknowledgement

SECTION 7: CERTIFICATION AND SIGNATURE PAGE

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, agree to comply with all mandatory requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

4Tellus LLC (Company)

941-228-2491
(Contact Phone/Fax Number)

Joseph Schnur, CCO
(Representative Name, Title)

1/24/2020
(Date)

Joseph Schnur
(Authorized Signature)

DESIGNATED CONTACT

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

Joseph Schnur, CCO
(Printed Name, Title)

941-228-2491

(Phone Number)/ (Fax Number)

800 Fairway Drive, Suite 360. Deerfield Beach, FL 33441

(Address)

Joe.Schnur@4tellus.com

(email address)

EXECUTIVE SUMMARY

Tellus is a leading U.S. provider of mobile Electronic Visit Verification (EVV) and claims processing technology designed especially for home health care. Tellus is solely focused on delivering best-in-class EVV solutions. We're proud to be the provider of choice for a variety of payers and agencies. Our comprehensive, cloud-based solutions work to simplify, streamline and accurately verify care tasks delivered to eligible recipients at the point of care, aggregate data from disparate sources, process service data, and generate claims that comply with the 21st Century Cures Act as well as defined policies and procedures. Our solutions help minimize fraud, waste, and abuse, and enable health care providers and caregivers to focus their efforts on what matters most — improved quality of service resulting in better outcomes, operational efficiency, ultimately, cost reduction.

Our highly configurable platform offers the flexibility to develop business rules and configuration settings to support the following DHHR EVV program goals and objectives:

- Enhance Accountability and Improve Quality of PCS and HHCS by:
  - Facilitating cost savings to DHHR and providers due to improved efficiencies and reduced paperwork
  - Enhancing the collection of data to assist DHHR in developing strategies to improve the quality of services and further prevent fraud, waste and abuse
  - Improving the effectiveness of PCS and HHCS provider administrative processes including improved support for billing and payment systems; scheduling; and documentation of service delivery
- Minimize Fraud, Waste and Abuse by:
  - Reducing inappropriately billed EVV-applicable services
  - Providing and electronic audit trail that accurately documents and tracks check-in and check-out times by EVV-applicable providers
  - Capture and identify visit, scheduling, and billing information to identify patterns of abuse, anomalies, and duplication of services
- Improve Reporting and Data Aggregation through Technology by:
  - Implementing an EVV system that facilitates a single composite view of home-based care delivery for improved data collection and integration
  - Automatically capturing and submitting claims with accurate dates of service; types of service; location of services; caregiver and recipient information and start and end time of services

- Enabling PCS and HHCS providers to easily report service delivery information in a timely manner

During the Solution Planning phase of the engagement Tellus' experienced EVV Implementation team will strive to gather and understand the details of each DHHR program to help determine the best way to comply with program requirements while achieving EVV program goals and objectives. We know each state is unique and many of the programs within each state must be configured differently in order to properly support members receiving services under those programs.

Tellus also recognizes the importance of stakeholder engagement. We have learned it is important to communicate with all stakeholders clearly and frequently to confirm their understanding of program goals and to alleviate fears and concerns constituents may have related to learning new technology and the invasion of privacy among other things. Getting the word out means engaging stakeholders in a variety of settings and timeslots to meet people where they are and allow them to be heard and understood.

Provider agencies are often concerned about payment of claims and whether they will be paid accurately and timely. Incorporating a soft launch into the implementation where provider agencies are required to use EVV but also have another mechanism for submitting claims can help alleviate these concerns. Tellus has experience with pilot programs and soft launches and can help DHHR construct this scenario if desired.

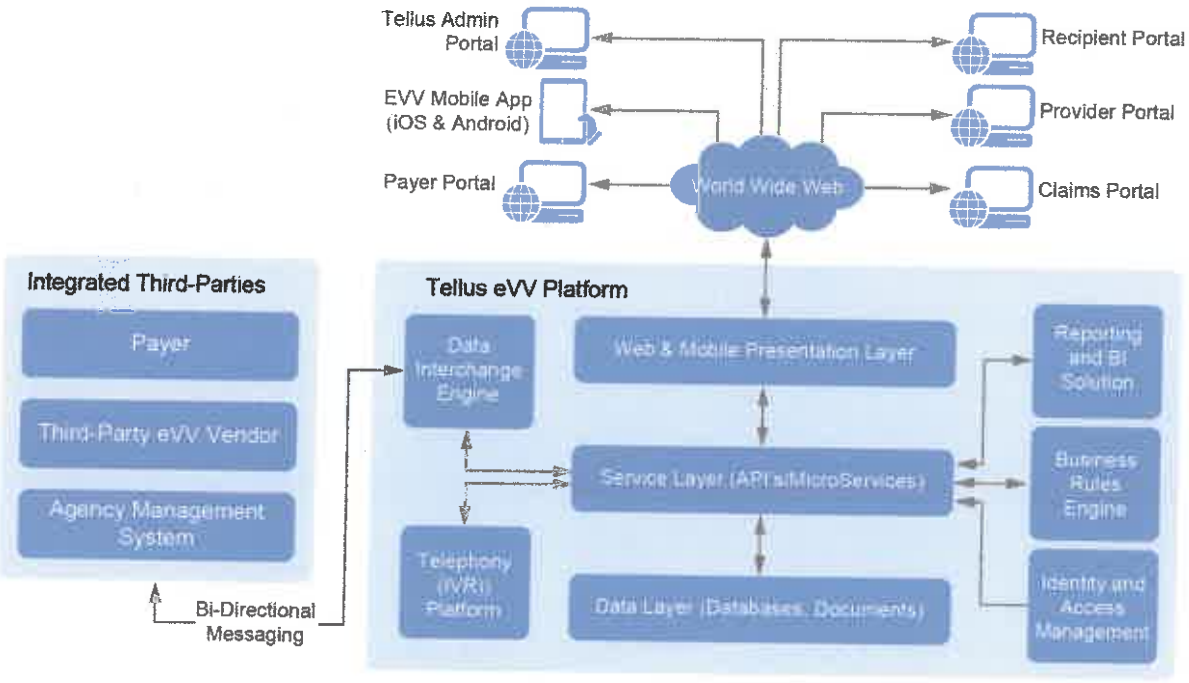
Tellus EVV is tried and true and operational supporting multiple EVV programs. Thousands of visits are completed using our platform each day. Completed visits are electronically, validated using rules specifically designed for each program. This pre-adjudication process, based on program-specific criteria, is one of the most valuable attributes of EVV. Visits are checked and validated. If they comply with program rules, they are seamlessly submitted to MMIS vendors to be adjudicated. If they do not comply with program rules, they must be reviewed and corrected prior to submission. After claims are adjudicated, they are either paid or denied. Providers are accurately paid for services rendered or notified to review noncompliant claims.

Because Tellus EVV is a Commercial-off-the-Shelf (COTS), Software-as-a-Service (SaaS) solution, the core components of our solution are already designed and developed. Instead of time-consuming, custom programming, our solution primarily requires configuration based on specific West Virginia requirements, as our draft project plan indicates, this can be accomplished within DHHR's six-month implementation timeline.

The Tellus EVV solution is comprised of five modules.

MODULE	PRIMARY FUNCTION
EVV Provider and Payer Consoles	Web-based consoles displaying real-time, dashboard-style overview of important metrics as well as the navigational menu for all other web-based user accessible components of the application including: administrative settings and functions, scheduling, claims processing, and reports. Users can access the consoles via web browsers (Chrome, Firefox, Safari, Internet Explorer, etc.).
EVV Mobile App	Android and iOS native applications downloaded and updated to user devices through commercial app stores, (with the ability to deploy and manage using enterprise management software for company-owned devices). The Tellus EVV Mobile App offers caregivers the convenience of using just one mobile device and app to verify scheduled visits on behalf of multiple agencies and payers. Caregivers remotely access their schedule and electronically confirm rendered services real-time.
EVV Claims Console	Web-based provider level pre-adjudication review of rendered services compared to payer authorized services and scheduled services. All transactions are run through business rules and matching logic then queued for review. Claims must meet payer requirements before they can be released by the provider to the payer for adjudication.
Business Rules Engine	Business rules are initially defined by the payer during the requirements gathering phase of the engagement and set up in the EVV rules engine. Rules are separate from the code base making them configurable and easy to change without development resources at the payer, program, provider and recipient level. Rules can be written around any field making our rules engine extremely robust and flexible.
Data Aggregation	Data integrity is the key to any successful program. Data is collected from third parties including payers, providers and third-party EVV vendors to assemble a complete data set for comprehensive claims submission, analytics and reporting purposes. Data imports can be scheduled at any desired frequency up to real-time.

The following diagram is a high-level architectural overview of the Tellus EVV Platform and how it interacts with integration partners and other users. Integrated third parties share information with Tellus EVV as directed by DHHR through Data Aggregation. Our Business Rules Engine applies program rules to manage data in accordance with DHHR guidelines. Users view and or enter data by accessing Tellus EVV using commercially available computers or smart phones.



The EVV Mobile App, EVV Administrator Console, and EVV Claims Console are fully integrated, intuitive and user friendly. The Data Aggregation and Business Rules engine allows seamless integration with disparate existing systems, such as West Virginia's Medicaid Management Information System (MMIS), as well as automatic analysis of data. Tellus is also a valued Optum teaming partner. Tellus and Optum have collaborated on a number of proposals. Optum excels at providing the data analytics and aggregation of data, as demonstrated through their data warehouse solution. In our teaming scenarios, Optum supports the analytic/aggregation solution, while Tellus supports the direct to provider solution.

The Tellus EVV platform is safe, simple, and cost-effective for payers and agencies to deploy and for caregivers to adopt.

The Tellus EVV solution is a modern, innovative platform designed to operate within the regulatory environment while continuing to promote the health, independence and community-living goals of individuals receiving services. The solution is compliant with a wide range of security and health information policies and protocols, including, but not

limited to HIPAA, FIPS, NIST cryptographic standards, FedRAMP, ISO 9001, HITECH, PCI DSS, as well as SOC 1, 2, and 3.

At Tellus, our mission is to develop long-term, trusted relationships with our clients through demonstrated performance and high-quality service delivery combined with a sincere desire to "do the right thing" for our clients and their participants each and every time. We take a balanced, holistic approach to solving business challenges, recognizing that each solution must combine aspects of strategy, process optimization, people and technology product innovation.

ATTACHMENT 3: VENDOR QUALIFICATIONS AND EXPERIENCE

Instructions: Organizational Overview: This section of the Vendor's Technical Proposal should include details of the Vendor and subcontractor overview. The Vendor's Technical Proposal should include organization overview, corporate background, Vendor's experience in public sector, and certifications. **Vendor Overview:** Provide all relevant information regarding the general profile of the Vendor.

1 ORGANIZATION OVERVIEW

Table 18: Vendor Overview

Vendor Overview	
Company Name	4Tellus, LLC
Name of Parent Company	N/A
Industry (NAICS)	541511
Type of Legal Entity	LLC
Company Ownership	Private
Number of Full Time Employees	52
Last Fiscal Year Company Revenue	$2M
Last Fiscal Year Company Net Income	$(5.7)M
% of Revenue from State and Local Government Clients in the United States	61%
% of Revenue from IT Design and Implementation Services	21%
Number of Years in Business	Seven
Number of Years the Vendor has Been Providing the Type of Services Specific in the RFP	Seven
Headquarters in the United States	Deerfield Beach, FL
Locations in the United States	Deerfield Beach, FL

Tellus will not be engaging Subcontractors to fulfill the requirements of this commitment. The Subcontractor Overview section is not applicable.

2 MANDATORY QUALIFICATIONS

Instructions: This section details the mandatory qualifications. The Vendor must complete this section to demonstrate that it has the experience needed to meet the requirements set forth in this RFP. Table 20: Mandatory Qualification below lists each mandatory qualification, the Vendor must note whether it meets the qualification and provide narrative demonstrating fulfillment of the requirement. The vendor must list each project experience separately and completely every time it is referenced.

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.	Tellus has had experience within the last three (3) years as the prime contractor for at least three (3) entities where the proposed solution has been implemented or is currently being implemented in an engagement of similar size and scope including the State of Florida Behavior Analysis program, United Healthcare Florida MCO and Aetna Florida MCO.
The Vendor must demonstrate at least three (3) years experience in Medicaid and Health and Human Services.	Tellus has over three (3) 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	References included in Section 5, below.

currently or has been implemented. Note, because this is a mandatory requirement, it will not be scored.	
The solution proposed by the Vendor must have been previously implemented successfully in a State environment.	Tellus EVV has been previously and successfully implemented in a State environment.
The Vendor must have at least three (3) years' experience in the operation of the proposed solution with similar size and scope to the State's in compliance with all Federal State regulations.	Tellus EVV has been operational with the Agency for Healthcare Administration, (AHCA) in the State of Florida for over three (3) years. Tellus is in compliance with all Federal and State regulations.

3 Existing Business Relationships with the State

Instructions: 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 States counties, and/or the states local municipalities.

Tellus has never had any relationships with the State of West Virginia or any State agencies.

4 Business Disputes

Instructions: 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 and phase of this project, each of these entities will submit this information as part of the response.

None.

5 REFERENCES

Instructions: 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.

Vendor (Prime) Reference Form:

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.

The Vendor should provide three (3) different clients/projects in order to demonstrate its experience.

Vendor should include project description, contract dates, and contact information (customer points of contact, addresses, telephone numbers and email addresses).

The Vendor should explain whether it performed the work as a prime contractor or as a subcontractor.

The Vendor should provide a response using **Table 21: Vendor References**. The Vendor my add additional Reference Tables as necessary.

Table 21: Vendor References

Reference 1

Vendor Information	
Vendor Name: 4Tellus LLC	Contact Name: Joe Schnur
	Contact Phone: 941-228-2491
Customer Information	
Customer Organization: Anthem, Inc	Contact Name: Lauren Fisher
	Contact Title: Program Director

Customer Address: 220 Virginia Avenue Indianapolis, IN 46204	Contact Phone: (303) 579-1321 Contact Email: lauren.fisher@anthem.com
Project Information	
Total Vendor Staff:	5
Project Objectives: To provide support with regards to the CURES act in implementing electronic visit verification and ongoing EVV services.	
Project Description: Provide EVV services for Anthem, Inc and their contracted Providers	
Vendor's Involvement: EVV Vendor (SaaS Vendor)	
Project Benefits: Provides a method of compliance with a configurable system for Anthem with regards to the CURES act.	
Key Personnel:	
Name: Joseph Schnur	Role: Account manager
Name: Irlande Germain	Role: Project Manager
Name: Christopher Pernicano	Role: Technical Manager
Project Measurements:	
Estimated one-time costs: Confidential not disclosable	Actual one-time costs: Confidential not disclosable
Reason(s) for change in one-time cost: No change from estimated one-time cost to actual one-time cost.	
Original Value of Vendor's Contract: Confidential not disclosable	Actual Total Contract Value: Confidential not disclosable
Reason(s) for change in value:	

There is no change in value from original value to actual value. Pricing does not change.				
Estimated Start & Completion Dates:	From: 11/1/2019		To: 12/31/2021	
Actual Start & Completion Dates:	From: 11/1/2019		To: On going	
If the Vendor performed the work as a Subcontractor, the Vendor should describe the scope of subcontracted activities: N/A				

Reference 2

Vendor Information	
Vendor Name: 4Tellus LLC	Contact Name: Joe Schnur
	Contact Phone: 941-228-2491
Customer Information	
Customer Organization: United Healthcare	Contact Name: Lori Hairston
	Contact Title: Assoc. Executive Director
Customer Address: 3100 SW 145th AVE, SUITE 200, MIRAMAR, FL 33027	Contact Phone: 954-364-0726
	Contact Email: lori_hairston@uhc.com
Project Information	

Total Vendor Staff:			5	
Project Objectives: To provide support with regards to the CURES act in implementing electronic visit verification and ongoing EVV services.				
Project Description: Provide EVV services for United Healthcare and their contracted Providers				
Vendor's Involvement: EVV Vendor (SaaS Vendor)				
Project Benefits: Provides a method of compliance with a configurable system for United Healthcare with regards to the CURES act.				
Key Personnel				
Name: Joseph Schnur			Role: Account Manager	
Name: Irlande Germain			Role: Project Manager	
Name: Christopher Pernicano			Role: Technical Manager	
Project Measurements:				
Estimated one-time costs: Confidential not disclosable			Actual one-time costs: Confidential not disclosable	
Reason(s) for change in one-time cost: No change from estimated one-time cost to actual one-time cost.				
Original Value of Vendor's Contract: Confidential not disclosable			Actual Total Contract Value: Confidential not disclosable	
Reason(s) for change in value: There is no change in value from original value to actual value. Pricing does not change.				
Estimated Start & Completion Dates:	From: 8/2018		To: Ongoing	

Actual Start & Completion Dates:	From: 8/2018		To: Ongoing	

If the Vendor performed the work as a Subcontractor, the Vendor should describe the scope of subcontracted activities:
N/A

Reference 3

Vendor Information	
Vendor Name: 4Tellus LLC	Contact Name: Bradley Levine
	Contact Phone: 954-461-8185
Customer Information	
Customer Organization: Agency for Health Care Administration	Contact Name: Toby Philpot
	Contact Title: AHCA Chief of Staff
Customer Address: 2727 Mahan Drive Tallahassee, FL 32308	Contact Phone: 850-421-3600
	Contact Email: toby.philpot@ahca.myflorida.com
Project Information	
Total Vendor Staff:	25
Project Objectives: We have two projects with AHCA: We provide support with regards to the CURES act in implementing electronic visit verification and ongoing EVV services for fee-for-service. And we provide behavioral analysis services for fraud waste and abuse.	

Project Description: Provide EVV services for ACHA and their contracted Providers				
Vendor's Involvement: EVV Vendor (SaaS Vendor)				
Project Benefits: Provides a method of compliance for ACHA with regards to the CURES act and provide fraud waste and abuse solution for behavioral analysis.				
Key Personnel				
Name: Bradley Levine	Role: Account Manager			
Name: Irlande Germain	Role: Project Manager			
Name: Christopher Pernicano	Role: Technical Manager			
Project Measurements:				
Estimated one-time costs: Fee-for-service: $769,691 Behavioral analysis: $625,000	Actual one-time costs: Fee-for-service: $769,691 Behavioral analysis: $625,000			
Reason(s) for change in one-time cost: No change				
Original Value of Vendor's Contract: Fee-for-service: $3,196,001 Behavioral analysis: $1,385,000	Actual Total Contract Value: Fee-for-service: $3,196,001 Behavioral analysis: $1,385,000			
Reason(s) for change in value: No Change				
Estimated Start & Completion Dates:	From: 11/1/2017		To: Ongoing	
Actual Start & Completion Dates:	From: 11/1/2017		To: Ongoing	

If the Vendor performed the work as a Subcontractor, the Vendor should describe the scope of subcontracted activities: Fee-for-service work is as a subcontract and behavioral analysis is direct for the state.

References for Subcontractor are not applicable, Tellus will not be utilizing the services of Subcontractors.

6 FINANCIAL STABILITY

Instructions: The Vendor should provide the following components for this section:

Dun & Bradstreet (D&B) Ratings. The Vendor should provide the industry standard D&B ratings that indicate its financial strength and creditworthiness, assigned to most U.S. and Canadian firms 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 that contain the firm's financial statement and credit payment history.

Please find the extract of Tellus' current D&B report below:

Build: 598

Welcome, Joel ▼

1.800.700.2733 Sign Out

Selected Company: TELLUS, LLC
D-U-N-S #: 05-167-3053

Overview

Business Summary

Company Name:	4TELLUS, LLC	
D-U-N-S #:	05-167-3053	
DBA's:	(FORMERLY: TELLUS, LLC),TELLUS	
Address:	800 Fairway Dr Ste 360	
City:	Deerfield Beach	
State:	FL	
Zip:	33441	
Phone:	9547190004	
Principal:	BRADLEY LEVINE	
Year Started:	2013	
Employs:	44 which includes officer(s).	
SIC Code(s):	73710302	Software programming applications
NAICS Code(s):	541511	Custom Computer Programming Services
Legal Structure:	N/A	

Special Events

08/12/2019 - Business name changed from Tellus, LLC to 4Tellus, LLC.

History and Operations

Officers and Directors

Current Officers

Name	Title
BRADLEY LEVINE	CEO
LIA SWEENEY	CFO
JOE SCHNUR	CHIEF CUSTOMER OFFICER
CHRIS PERNICANO	COO

Current Directors

Name
BRADLEY LEVINE
LIA SWEENEY
JOE SCHNUR

CHRIS PERNICANO

Company History

Provides computer programming services, specializing in software programming applications (100%).

Operations

Employees

44 which includes officer(s).

Facilities

Rents 1,500 sq. ft. on 4th floor of a four story cinder block building.

Location

There is currently no location information listed in this company report.

U.S. Branch

There are currently no U.S. branches listed in this company report.

U.S. Subsidiary

There are currently no U.S. subsidiaries listed in this company report.

International Branch

There are currently no international branches listed in this company report.

International Subsidiary

There are currently no international subsidiaries listed in this company report.

Payments

Payment Summary

	Total Received	Total Dollar Amount	Largest High Credit Payment summary	Within Terms	Days Slow <31	31-60	61-90	91+
Top Industries								
Help supply service	1	$15,000	$15,000	100%	0	0	0	0
Natnl commercial bank	1	$5,000	$5,000	100%	0	0	0	0
Trucking non-local	1	$500	$500	100%	0	0	0	0
Reg misc comi sector	1	$250	$250	100%	0	0	0	0
Electric services	1	$250	$250	100%	0	0	0	0
Other Categories								
Cash experiences	8	$500	$100					
Unknown	0	$0	$0					
Unfavorable comments	0	$0	$0					

	Total Received	Total Dollar Amount	Largest High Credit Payment summary	Within Terms	Days Slow <31	31-60	61-90	91+
Placed for collections with D&B:	0	$0	$0					
Other	0	N/A	$0					
Total in D&B's file	13	$21,500	$15,000					

The highest Now Owes on file is $15,000

The highest Past Due on file is $0

There are 13 payment experience(s) in D&Bs file for the most recent 24 months, with 6 experience(s) reported during the last three month period.

Payment Details

Total (Last 24 Months): 13

Date ◆	Paying Record	High Credit	Now Owes	Past Due	Selling Terms	Last sale within (Mo.)
12/2019	(001)	$100	--	--	Cash account	4-5 mos
11/2019	Ppt	$15,000	$15,000	$0	N30	1 mo
11/2019	(003)	$0	$0	$0	Cash account	6-12 mos
10/2019	(004)	$100	--	--	Cash account	1 mo
10/2019	(005)	$50	--	--	Cash account	1 mo
10/2019	(006)	$50	--	--	Cash account	1 mo
07/2019	Ppt	$500	$0	$0		6-12 mos
06/2019	(008)	$100	--	--	Cash account	1 mo
04/2019	(009)	$50	--	--	Cash account	1 mo
12/2018	Ppt	$5,000	$250	$0		1 mo
08/2018	(011)	$250	--	--		1 mo
06/2018	Ppt	$250	$0	--		6-12 mos
05/2018	(013)	$50	--	--	Cash account	1 mo

Payments Detail Key: ■ 30 or more days beyond terms

Accounts are sometimes placed for collection even though the existence or amount of the debt is disputed.

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.

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

Finances

Key Financial Comparisons

This Company's Operating Results Year Over Year

Net Sales	NA	NA	NA
Gross Profit	NA	NA	NA
Net Profit	NA	NA	NA
Dividends / Withdrawals	NA	NA	NA
Working Capital	NA	NA	NA
This Company's Assets Year Over Year			
Cash	NA	NA	NA
Accounts Receivable	NA	NA	NA
Notes Receivable	NA	NA	NA
Inventories	NA	NA	NA
Other Current	NA	NA	NA
Total Current	NA	NA	NA
Fixed Assets	NA	NA	NA
Other Non Current	NA	NA	NA
Total Assets	NA	NA	NA
This Company's Liabilities Year Over Year			
Accounts Payable	NA	NA	NA
Bank Loan	NA	NA	NA
Notes Payable	NA	NA	NA
Other Current	NA	NA	NA
Total Current	NA	NA	NA
Long Term Debt	NA	NA	NA
Deferred Credit	NA	NA	NA
Net Worth	NA	NA	NA
Total Liabilities And Net Worth	NA	NA	NA

Balance Sheet

Fiscal Consolidated Statement Dated

We currently do not have any recent financial statement on file for this business.

Key Business Ratios

(Industry Median is based on this number of firms:)

Solvency			
Quick Ratio	NA	NA	NA
Current Ratio	NA	NA	NA
Current Liabilities to Net Worth	NA	NA	NA
Current Liabilities to Inventory	NA	NA	NA
Total Current	NA	NA	NA
Fixed Assets to Net Worth	NA	NA	NA
Efficiency			
Collection Period	NA	NA	NA
Inventory Turn Over	NA	NA	NA
Sales to NWC	NA	NA	NA
Acct Pay to Sales	NA	NA	NA
Profitability			
Return on Sales	NA	NA	NA
Return on Assets	NA	NA	NA
Return on NetWorth	NA	NA	NA

Public Filings

Summary

This following public filing data includes both open and closed filings found in D&B's database on this company. It is for informational purposes only and is not the official record. Certified copies can be obtained from the official source.

Record Type	# of Records	Most Recent Filing Date
UCC Filing	1	05/17/0019
Government History	1	N/A

Details

Judgements

No judgments have been reported to D&B on this company.

Liens

No liens have been reported to D&B on this company.

Bulk

No suits have been reported to D&B on this company.

UCC Filings

Collateral:	All Assets including proceeds and products
Type:	Original
Secured Party:	CIBC BANK USA, CHICAGO, IL
Debtor:	4TELLUS, LLC
Filing Number:	2019 2781289
Filed With:	
Date Filed:	04/22/19
Latest Info Received:	05/17/19
Original Filing Number:	
Original UCC Filed Date:	

Bankruptcies

No bankruptcies have been reported to D&B on this company.

Government History

Borrower(Dir/Guar):	NO
Administrative Debt:	NO
Contractor:	NO
Grantee:	NO
Party excluded from federal program(s):	NO
Labor Surplus Area:	N/A
Small Business:	YES (2019)
8(A) Firm:	N/A

Privacy Policy | Terms of Use

ATTACHMENT 4: PROJECT ORGANIZATION AND STAFFING APPROACH

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). 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. For ease of formatting and evaluation, Attachment 4: Project Organization and Staffing Approach provides the required outline for the Vendor's response to staffing. The Vendor's response to the following should not exceed 25 pages, excluding key personnel resumes and the forms provided in this Attachment. Refer to request for proposal (RFP) ***Section 4.7.1 Qualifications and Experience*** for the details pertaining to staff qualifications, experience, and responsibilities.

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.

3.2.1 To ensure successful transition to the operations phase, the implementation activities should be led by key staff identified in the list below:

3.2.1.1 Account Manager

3.2.1.1 Project Manager

3.2.1.1 Quality Assurance Manager

3.3.1 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.

Table 8: Staff Qualifications, Experience, and Responsibilities

VENDOR ROLE	QUALIFICATIONS	RESPONSIBILITIES
Account Manager	A minimum of eight (8) years of demonstrated experience in: a. Management of an organizational unit within a Human Services Department in a U.S. state or territory; and/or b. Management of an organizational unit within a Human Services Department that is performing operations in a state similar in scope to the services that the State of West Virginia has requested: and/or c. Experience in another healthcare Electronic Visit Verification (EVV) setting or agency contracted with the state/territory responsible for the performance of the same. d. Must have a Master of Business Administration (MBA), Master of Health Administration (MHA), Master of Public Administration (MPA), other advanced business degree, or comparable work experience. e. Must have demonstrated	The Account Manager shall be assigned to the project on a full-time basis for the duration of the contract. The Account Manager shall be the single point of contact for the duration of the contract and is responsible for: 1. Contracting oversight from start-up through the life of the contract. 2. Attending in person, upon DHHR's request, meetings and hearings of legislative committees and interested governmental bodies, agencies, officers, providers, and stakeholders. 3. Meeting with DHHR staff or such other person as DHHR may designate on a regular basis to provide oral and written status reports and other information as required. **Note:** DHHR will approve the initial Account Manager and any changes *to* a different Account Manager over the life of the contract.

	knowledge of the Medicaid policy and administrative rules governing fee-for- service modules. f. Must have demonstrated knowledge of EVV systems and Medicaid claims processing. g. Must have a demonstrated knowledge of the delivery of home- and community-based services.	
Project Manager	a. Project Management Professional Certification. b. A minimum of five (5) years of experience in project management of an information technology (IT) project(s) that encompassed the system development in duration, scope, and complexity to the EVV project.	The Project Manager shall be assigned to the project on a full-time basis for the duration of the development and implementation work, until the EVV system is successfully implemented and accepted by DHHR. The Project Manager is responsible for all project management activities and for ensuring all project requirements are satisfied, including: 1. Attending in person, upon DHHR request, meetings and hearings of legislative committees and interested governmental bodies, agencies, officers, providers, and stakeholders. 2. Maintaining the project plan over the life of the project. 3. Supporting any federal gatepost reviews, including

		Centers for Medicare & Medicaid Services (CMS), State, and or federal certification processes. **Note:** DHHR will approve the initial Project Manager and any change to a different Project Manager over the life of the contract.
Quality Manager	a. Bachelor's degree, preferably in healthcare administration, nursing, health information administration, or comparable work experience. b. A minimum of four (4) years of experience serving as Quality Manager for projects similar in size, duration, and complexity to the EVV project. c. A minimum of three (3) years of experience in claims processing and data management.	The Quality Manager will be the single point of contact for the EVV system, and is responsible for: 1. Management of theday-to-day operation of the EVV system, including issue management and resolution. 2. Attending in person, upon DHHR request, meetings and hearings of legislative committees and interested governmental bodies, agencies, officers, providers, and stakeholders. 3. Managing all test activities related to the development and implementation of the EVV system.

		Note: DHHR will approve the initial Quality Manager and any changes to a different Quality Manager over the life of the contract.

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.

Table 23: Resumes for Proposed Key Staff

NAME	PROPOSED ROLE	EXPERIENCE IN PROPOSED ROLE
Joseph Schnur	Account Manager	+20 years
Irlande Germain	Project Manager	9 years
Maria Bojko	Quality Assurance Manager	6 years

STAFF RESUMES: ACCOUNT MANAGER

JOSEPH M. SCHNUR

Fort Lauderdale, FL

Cell: 941-228-2491 ▪ jschnur1@verizon.net ▪ linkedin.com/in/joeschnur

C-LEVEL BUSINESS EXECUTIVE

► ***PLAYING TO WIN and not just compete by relentlessly focusing on constant improvement*** ◄

Pioneering, game-changing and entrepreneurial ***C-Level Business Executive*** offering progressive and diverse commercial and operational experience spanning Fortune 100 to start-up organizations. Inspirational leader who can build, coach and mentor high performance teams, and cultivate strong relationships with key stakeholders. Excel at aligning strategy with tactical execution to drive new product innovation, launch go-to-market initiatives, deliver explosive growth, and boost profitability. Proficient at connecting the dots and strategically managing multiple priorities. Add enterprise value utilizing active listening, intellectual curiosity, insightful business judgment, a customer-centric focus, and an unwavering level of ethics and integrity.

APPLIED SKILLS & KNOWLEDGE

- Strategic Planning
- Start-Ups
- P&L Management
- Project Management
- Change Management
- Product Strategy & Innovation
- Product Marketing
- Market Analysis
- Business Development
- Process Improvement
- Needs Assessment
- Relationship Management
- Talent Acquisition
- Complex Negotiations
- Training & Development

PROFESSIONAL EXPERIENCE

Tellus - Deerfield Beach, FL ▪ 2018 – Present

Private equity backed provider of mobile care delivery, Electronic Visit Verification (EVV) and claims processing technology.

Chief Customer Officer

Senior executive (acting as COO/CRO/Chief Strategy Officer) supporting CEO (company Founder). Conceive and lead commercial go-to-market, client acquisition, business development, and product strategy. Identify market opportunities by analyzing industry trends, generating competitive intelligence and assessing/prioritizing growth targets. Oversee sales, strategic partnerships and provider implementations for approximately 100 new deals/month.

- Transformed sales team including inside sales and account management into a high-performance group; designed onboarding process and sales training program to accelerate learning curve.
- Spearheaded organic revenue growth from $1 million in annual recurring revenue (ARR) and one commercial contract to $8 million and more than 1,000 contracts (including four state and six MCO contracts).
- Increased monthly sales volume by 400% through strategic partnerships and effective program communications.
- Gained 60% market share in Florida market by booking 1,000 new provider contracts with home health agencies.
- Contracted with enterprise brands including United Healthcare, Anthem, Aetna, Verizon, Sprint, and Optum.
- Originated EVV clearinghouse product strategy that has become the company's core offering and key differentiator.
- Implemented multiple SOPs to drive more efficient decision making, communication and project execution.

CareThrough - Bradenton, FL ▪ 2016 – 2017

Provider of staff in hospitals and practices; portfolio company of HealthChannels, private equity backed $250 million business.

Founder & President

Directed all business functions including solution development, marketing, pricing, sales, partnerships, contracting, implementation, training, and operations. Partnered with multiple technology companies.

- Piloted new business unit from concept to $2 million in annual recurring revenue (ARR) in year one.

Valence Health - Chicago, IL ▪ 2014 – 2016

Private equity backed high growth technology and services business.

Vice President of Business Development

Led business strategy, product development, pricing, and solution delivery.

- Generated 6x organic growth in revenue that resulted in successful acquisition by Evolent Health.

Intelligent M - Bradenton, FL ▪ 2013 – 2014

Private equity startup providing wearable technology and a social networking application to improve hand hygiene behaviors.

Chief Commercial Officer

Launched commercial business by developing target markets and segmentation, solution design, value proposition, pricing, client pitches, and brand messaging. Designed and implemented marketing strategy and lead generation program. Oversaw client acquisition, sales, contracting, deal closure, account management, global distribution and sales agent development.

- Drove sales growth from concept to $2 million in annual recurring revenue (ARR).
- Redesigned pricing model and prioritized product roadmap based on voice of the customer (VOC) and usage.
- Championed product simplification that increased profitability by 80% and reduced implementation time by 500%.
- Created innovative charging station that boosted product performance and enhanced the customer experience.
- Devised a mobile application that gamified the product solution and increased client engagement by 90%.
- Invented disposable wrist bands with customization to eliminate the largest product pushback voiced by clients.

General Electric Company/GE Healthcare - Chicago, IL ▪ 1996 – 2012

Enterprise General Manager - (2004 – 2012)

Led 15-person team across the US to support HCA (GE Healthcare's largest client) with responsibility

for annual equipment, service and solutions revenue exceeding $400 million annually.

- Reengineered the sales model, hiring process and compensation plan; created a vision that inspired internal and external alignment, defined success metrics and drove execution with strong operating rigor.
- Instituted enterprise account management and aligned KPIs to create a unique value proposition, resulting in stronger client loyalty, contracts with 95% commitment levels and 90% market share (3x the national average).
- Built a customer-centric, solutions-oriented culture that encouraged creative thinking and continuous learning.
- Forged collaborative client partnerships that sparked joint development of new products and solutions.
- Created messaging and produced internal commercial video for GE's Healthymagination initiative.
- Designed product concept for business analytics software and led M&A with RFID business.

Corporate Account Manager (2002 – 2004)

Handled all sales and account relationship activities for a large hospital system across Florida, Georgia and South Carolina.

- Established an enterprise sales approach that produced a major commercial shift within the organization and supported the closing of a $100 million deal.

Account Manager (1997 – 2001)

Served as commercial lead for radiology products and related service portfolio to 40 hospitals.

- Grew capital equipment orders from $4 million to $13 million and generated win-rate exceeding 90% by securing several strategic alliance agreements and converting multiple competitive accounts.
- Developed various strategic selling tools that were recognized as GE best practices.

Leadership Program (1996 – 1997)

Recruited as one of 12 college graduates per year into the company's ultra competitive rotational training program.

MILITARY EXPERIENCE

United States Navy, USS Theodore Roosevelt

Aviation Boatswain Mate, ABE-3 - Operated and maintained catapult systems on a naval aircraft carrier.

- Ensured compliance with all aircraft launching procedures 24 hours/day under extreme and dangerous conditions.
- Completed fire-fighting certification and received hazardous duty status for working on the flight deck.

EDUCATION & PROFESSIONAL DEVELOPMENT

Bachelor of Science (BS) in Mechanical Engineering, PENN STATE UNIVERSITY - University Park, PA

Multiple executive management/leadership/sales training courses, GE JACK WELSH CENTER FOR CORPORATE DEVELOPMENT

STAFF RESUMES: PROJECT MANAGER

IRLANDE GERMAIN, PMP

Miami, Florida

(317) 658-0208 ▪ irlande.germain@4tellus.com ▪

PROFESSIONAL EXPERIENCE

Tellus - Deerfield Beach, FL ▪ 2018 – Present

Growing company offering software products to healthcare providers and development services employing onshore and offshore resources. PMP Certified Project Manager, leading Tellus EVV software implementations, focusing on grand-scale, highly regulated, Electronic Visit Verification (EVV) software implementations for statewide government and MCO contracts.

Senior Project Manager

- Leads project management for large, complex EVV software implementations for statewide government and MCO contracts.
- Gathers requirements using project management and business analysis methodologies such as interviews, requirement workshops, use cases, workflow analysis, and document analysis.
- Develops detailed project plans, project timelines, reports, and project status sheets that are managed and disseminated throughout the project life cycle.
- Identifies and migrates risks/issues/blockers impeding project delivery.
- Manages stakeholder and leadership expectations throughout the project management lifecycle.
- Validates high level of compliance to HIPAA guidelines and protection of PHI.
- Defines IT project scope, goals, and deliverables that support business goals in collaboration with senior management and stakeholders.
- Champions grooming, iteration planning, organizing, and motivating teams to achieve a higher level of performance through value-driven practices.
- Performs system development life cycle (SDLC) activities using the Agile Scrum methodology phases from project initiation through project closure.

PAYBOX Corporation – Ft. Lauderdale, FL ▪ 2017 - 2018

Automation solutions for mid-Size to large enterprise companies and banks. Served as the lead project manager to lead AR & AP solutions that streamline and automate processes while providing financial visibility.

Lead Project Manager

- Planned, scheduled, tracked, and managed software development project timelines, milestones, and deliverables while developing detailed project plans and associated communication documents.
- Maintained effectiveness and efficiency by defining, delivering, and supporting strategic plans for implementation.
- Verified application results by conducting system audits of technologies implemented.
- Developed detailed project plans and associated communications documents.
- Worked with internal teams developing and validating schedules and plans/ gaining signoffs.
- Identified and managed project dependencies and critical path; delegated tasks and responsibilities to appropriate resources.
- Maintained master project documentation and project status reports; facilitated status meetings.
- Regularly reviewed project scope, costs, performance, and business benefits to keep the project on track; facilitated communication between functional groups; proactively managed changes in project scope, identified potential risks, and devised contingency plans
- Ensured change management; validated changes identified, validated, estimated; communicated impact of changes; ensured issues w/ managing processes were handled appropriately.
- Trained cross-functional team members on new processes, procedures, and tools to mitigate risk.
- Set and continually managed project expectations with team members and stakeholders.
- Identified and resolved issues and conflicts within the project team.
- Assisted sales teams with demonstration of software and with onsite training and development of training materials.

Homes Media Solutions – Boca Raton, FL ▪ 2013 - 2017

Combining several real estate media and technology brands, Homes Media Solutions specializes in marketing and data solutions for real estate professionals.

Project Manager

- Detailed requirements writing, prototyping, outlining project scope, developing project charter, and completing gap analysis; responsible for creating release plans.

- Contributed to the technical assessment, scope definition, project planning, analysis, design, implementation, and testing of large, complex projects.
- Conducted both internal and external meetings and documented meeting agendas, notes, and action items.
- Demonstrated strong verbal and written communication through effectively managing project updates, changes, and risks to stakeholders.
- Served as primary point of contact for enterprise customers and vendors.
- Led/supported many teams of 10-15 through grooming, planning, and execution of project scope.
- Managed and escalated defects within backlog during steady state.
- Consistently exceeded expectations by verifying projects were on time, within budget, with to standards, and met business needs.
- Created detailed build notices outlining deliverables and project highlights.
- Facilitated daily Scrum meetings and Agile board with cross-functional team members.
- Worked with stakeholders to lead the analysis, development, and standardization of processes and procedures to optimize successful project delivery.
- Navigated problems that arose during the project to senior management when necessary and provided resolutions.

Finish Line - Indianapolis, IN ▪ 2010 - 2013

Assistant Project Manager

- Transitioned to Assistant Project Manager; $15 million wide area network project after developing strategic techniques for resolving project issues.
- Provided project management for projects including hardware integrations, and software upgrades.
- Contributed to project plans, implementation plans, test plans, and functional requirements to confirm projects were completed on time and under budget.
- Increased productivity by developing manuals, runbooks, and department guides for both the network team and end-users.
- Consistently exceeded expectations validating projects were on time, within budget, compliant with standards, and met business needs; contributed to the technical assessment, scope definition, project planning, analysis, design, implementation, and testing of large projects.

American Funds Service Company - Indianapolis, IN ▪ 2005 - **2010**
Shareholder Service Account Representative

EDUCATION & CERTIFICATIONS

Indiana University - Bloomington, IN ▪ 2000-2004
Bachelor of Arts, General Studies

Project Management Professional - Project Management Institute ▪ 2017
PMP [redacted]

COMPTIA Network + - **COMPTIA A +** ▪ 2010

STAFF RESUMES: QUALITY ASSURANCE MANAGER

MARIA BOJKO

Margate, Florida

(561) 452-1465 ▪ mbojko@fau.edu ▪ https://www.linkedin.com/in/maria-bojko-9abb6688

C-LEVEL BUSINESS EXECUTIVE

A Quality Assurance Engineer with more than four years of experience with great attention to detail and a commitment to developing and implementing continuous improvement initiatives through the collection and analysis of data and converting it into actionable information. With full system development lifecycle experience, including designing, developing and implementing test plans, test cases and test processes.

APPLIED SKILLS & KNOWLEDGE

- **Frameworks:** .Net, Android UI kit, Node, React, Salesforce, Junit, Selenium
- **Test tools:** VMWare vSphere, Postman, Soap UI, Bugzilla, ATM, Test Complete, SNOW
- **Development methodologies:** Agile (scrum) Tools: Rally, Jira
- **Version control:** Git
- **Databases:** Postgres, Oracle SQL Developer, MySQL, MS SQL server

PROFESSIONAL EXPERIENCE

Tellus - Deerfield Beach, FL ▪ 2019 – Present

Lead QA Engineer

- Proposed technical solutions to issues encountered by customers that were simple to implement yet effective in their approach, saving company resources from costly refactors.
- Lead QA team at a high pace work environment across multiple projects with different roadmaps and requirements, aligning them to the company's overall needs.
- Debugged code alongside developers to find root cause of issues
- Used developer tools and postman to determine origination point of issues (UI, API and/or DB)
- Tested MySQL stored procedures and validated Database schemas against specifications.
- Performed Business Analysis functionalities along with my daily duties due to limited resources and high customer demands.
- Performed full system, integration and regression tests expanding multiple tiers in the System (UI layer, API layer, DB layer)
- Submitted high level proposal to automate Smoke/Critical tests leveraging Selenium and Junit along with a prototype.
- Highlighted Gaps in requirements that would lead to potential issues saving the company resources by not needing to address them later.
- Effectively worked and communicated with different team members across multiple countries and cultures.
- Context switched frequently during the days between projects, effectively managing workload and leading team as quickly changing priorities came in for different projects.

Lennar - Sunrise, FL

SR QA Tester ▪ Oct 2017 - Feb 2019

- (ETL testing) verified data integrity between transfer

- Developed mapping, and transformation scripts based on requirement/rules from Business Analysis
- Analyzed business process workflows and assisted in development of ETL procedures for moving data from source to target systems
- (Sales Force) analyzed use cases and requirements to develop test cases for inquiring permissions and functional testing across multiple devices
- Managed test suites for multiple in-house applications
- Took initiative and volunteered for critical projects in the company when others did not or could not.
- Supervised and guided multiple software QA testers on company projects.
- Reviewed test cases and conducted Peer reviews meetings with the team
- Provided detailed walkthrough of test plans and test cases to project team
- Logged and traced defects to closure using Jira and followed up with the BA and developers to discuss about the issues.
- Worked with the project manager to identify resources, scope and limitations of testing.
- Prepared and published test summary reports at the end of the day with results of readiness of system deployment to production environment
- Prepared weekly testing progress report and presented to onsite member and managers on the team

QA Contractor ▪ Mar 2017 - Oct 2017

- Tested data security sensitive web application on multiple platforms and verified implementation of infrastructure
- Provided QA service at all hours for Emergency testing and deployment
- Worked closely with project managers and developers to handle multiple priority projects simultaneously
- Develop and successfully executed detailed test plans, procedures and scenarios for unit, process, function, system integration, acceptance and regression testing.
- Worked within the full-lifecycle of software development including analyzing, designing, building, testing, implementing, agile and supporting applications

---

Emerson Network Power - Sunrise, Florida ▪ Jan 2015 - Jan 2017

QA Test Engineer

- Coordinated between development and customer to produce customer issue in an isolated testable environment and resolved field issues in a timely manner.
- Created and administered Virtual Machines for multiple test environment and managed snapshots to ensure integrity of testing environments.
- Created clear and concise test plans and test cases based on story requirements.
- Created and managed test session for QA team members for thorough coverage.
- Manage a team of five and available resources for efficient parallel testing under stick timeline.
- Worked closely with development throughout the lifecycle of a defect (detection, reporting, fix, deploy-fix, validation, close defect)
- Adapted quickly to changing criteria and technologies in Agile development. (Started testing SOAP and ADF GUI and transitioned to testing RESTful API and angular based GUI).
- Became efficient at noticing common development coding pitfalls and quickly caught common issues earlier in the testing cycle.

EDUCATION & CERTIFICATIONS

Florida Atlantic University - Boca Raton, FL ▪ 2011-2014
Bachelor of Science Computer Engineer

LANGUAGES

Fluent in English, Spanish

3.3 References

3.2.4 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.

3.2.5 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.

3.2.6 Vendors should use the format provided in **Table 24: Key Staff References.** Repeat the rows and tables as necessary.

Table 24: Key Staff References

KEY PERSONNEL REFERENCE FORM					
Key Personnel Name:	Joseph Schnur	Proposed Role:	Account Manager		
Reference 1					
Client Name:	Anthem	**Client Address:**	9250 W Flagler St, Suite 600, Miami, FL 33174		
Contact Name:	Lauren Fisher	**Contact Title:**	Program Director | GBD Segment & Product Mgt - LTSS		
Contact Phone:	(303) 579-1321	**Contact E-mail:**	lauren.fisher@anthem.com		
Project Name: FL & VA EVV		**Start Date:**	01/2019	**End Date:**	04/2020
Project Description: Implement EVV across provider network in FL & VA					
Project Role and Responsibilities: Project Leader overseeing implementation					

Reference 2							
Client Name:	United Healthcare	**Client Address:**					
Contact Name:	Lori Hairston	**Contact Title:**	Executive Director, Long Term Care Program				
Contact Phone:	(678) 591-3313	**Contact E-mail:**	lori_hairston@uhc.com				
Project Name: FL EVV				**Start Date:**	01/2019	**End Date:**	04/2020
Project Description: EVV Implementation across provider network in FL							
Project Role and Responsibilities: Executive sponsor for EVV implementation							
Reference 3							
Client Name:	GE	**Client Address:**					
Contact Name:	Alfredo Arguello	**Contact Title:**	General Manager				
Contact Phone:	(615) 585-5854	**Contact E-mail:**	Alfredo.arguello@ge.com				
Project Name: HCA				**Start Date:**	06/2004	**End Date:**	11/2012
Project Description: Strategic leadership with a nationally-based provider							
Project Role and Responsibilities: Executive sponsor and leader of team							

KEY PERSONNEL REFERENCE FORM

Key Personnel Name:	Irlande Germain	**Proposed Role:**	Project Manager

Reference 1

Client Name:	Joe Vosilla	**Client Address:**	500 E Broward Blvd, Ste 1150 Ft. Lauderdale, FL 33394
Contact Name:	Joe Vosilla	**Contact Title:**	Senior Director, Development and Delivery
Contact Phone:	(954) 510-3750	**Contact E-mail:**	joe.vosilla@gopaybox.com

Project Name: ERP System Integration	**Start Date:**	05/2017	**End Date:**	05/2018

Project Description: Work with customer to outline ERP system specifications and requirements for new AR/AP customer portal.

Project Role and Responsibilities: Map invoice data points to database fields, create prototypes, create requirements document, create and execute project schedule. Work with both development and QA teams to transition project through various stages. Work with customer on completing User Acceptance Testing. Create change orders as needed. Complete project closure.

Reference 2

Client Name:	Patrice Guthrie	**Client Address:**	1500 NW 136th Ave Sunrise, FL 33323
Contact Name:	Patrice Guthrie	**Contact Title:**	Product Owner

Contact Phone:	(954) 503-0282	**Contact E-mail:**	Patrice.guthrie@aexp.com		
Project Name: RE/MAX of Western Canada Broker portal			**Start Date:** 07/2014	**End Date:**	05/2017
Project Description: Worked with customer to deliver a CRM/Marketing tool for all brokers contracted under Re/Max of Western Canada					
Project Role and Responsibilities: Gather requirements, work with the development and integrations team to transmit data from MSL boards to internal databases. Manage schedule and conduct risk management and stakeholder management tasks. Manage scrum teams to release features in two-week sprint cycles. Lead sprint demos for customer and create change orders based on demo feedback when necessary. Drive user-acceptance testing and finally close out project.					
Reference 3					
Client Name:	Cyndi Edwards	**Client Address:**	999 Yamato Rd, Suite 200 Boca Raton, FL 33487, US		
Contact Name:	Cyndi Edwards	**Contact Title:**	Manager of Project Management		
Contact Phone:	877-363-4442	**Contact E-mail:**	cyndi.edwards@homes.com		
Project Name: Homes Connect			**Start Date:** 07/2014	**End Date:**	05/2017
Project Description: Scrum master working with team to deliver enhancements and features for the company's core product.					
Project Role and Responsibilities: Work with product team to refine backlog. Write user-stories and create prototypes. Work with the scrum team to groom, plan, execute features within the sprint cycle. Lead sprint demo and retrospective meetings. Interface with overseas teams and co-working teams on a daily basis as part of managing task progression. Create weekly reports for management and customers.					

KEY PERSONNEL REFERENCE FORM			
Key Personnel Name:	Maria Bojko	Proposed Role:	Quality Assurance

Reference 1			
Client Name:	Clarence Davis	**Client Address:**	Veritiv 500 W Cypress Creek Rd, Fort Lauderdale, FL 33309
Contact Name:	Clarence Davis	**Contact Title:**	Staff Engineer
Contact Phone:	954-628-0500	**Contact E-mail:**	Clarence.Davis@vertiv.com

Project Name: Trellis	**Start Date:**	02/2014	**End Date:**	01/2017
Project Description: DCM Monitoring				
Project Role and Responsibilities: Quality Assurance				

Reference 2			
Client Name:	Perry Francis	**Client Address:**	Veritiv 500 W Cypress Creek Rd, Fort Lauderdale, FL 33309
Contact Name:	Perry Francis	**Contact Title:**	Software Engineer
Contact Phone:	954-746-9000	**Contact E-mail:**	Perry.Francis@vertiv.com

Project Name: Trellis		**Start Date:**	02-2014	**End Date:**	01-2017
Project Description: DCM Monitoring					
Project Role and Responsibilities: Developer					
Reference 3					
Client Name:	Mathew Itty	**Client Address :**	Veritiv 500 W Cypress Creek Rd, Fort Lauderdale, FL 33309		
Contact Name:	Mathew Itty	**Contact Title:**	Quality Assurance Manager		
Contact Phone:	(561) 226-4441	**Contact E-mail:**	mathew.Itty@vertiv.com		
Project Name: Trellis			**Start Date:**	02/2014	**End Date:** 01/2017
Project Description: DCM Monitoring					
Project Role and Responsibilities: QA Manager					

ATTACHMENT 5: INITIAL WORK PLAN

Instructions: The Vendor should provide an Initial Work Plan. At a minimum, the Vendor's proposed Initial Work Plan *should include* the following:

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:

- Responsibilities
- Timelines and Durations
- Milestone Dates
- Deliverable Dates
- Vendor personnel hours by deliverables for each project phase
- Department of Health and Human Resources (DHHR) personnel hours by phase deliverable
- All critical dependencies for the project's milestones and deliverables

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)

Project Schedule for all project deliverables and milestones

Identification of resources assigned the responsibility for each deliverable within the WBS to the level at which control will be exercised

Identification of deliverables that require a more-prompt DHHR acceptance than described in the RFP, including the proposed acceptance period for the deliverable

The Initial Work Plan should be provided as an attachment to the Vendor's Technical Proposal and tabbed as such in the submission.

1 INITIAL WORK PLAN

Tellus aligned the draft of our initial work plan with the milestones and deliverables outlined by DHHR in the RFP document. Our detailed West Virginia Draft Project Schedule is contained in this response as Addendum A.

The project schedule incorporates all of the tasks identified by DHHR as project milestones and deliverables with an estimated timeline and duration for each. The project schedule began with a project start date of 3/2/2020, referenced herein as Contract Award. Tellus estimates one month will elapse between Contract Award and Contract Execution. All durations specified in the table below are in days and referenced in relation to Contract Execution. The number of days indicated is based on how long the deliverable is estimated to be complete factoring in submission of draft to DHHR, their review, Tellus revisions, DHHR review of revisions and approval of final plan.

The actual Milestone and Deliverable dates depend upon the date of contract award and execution. Tellus is confident in our ability to implement and transition the solution to DHHR in six (6) months after the contract is executed.

In addition, the following table extends that information to include the primary Tellus resource who will be responsible for supporting the Tellus Project Manager to ensure the related project deliverable is completed in accordance with DHHR guidelines both timely and accurately. The Tellus Project Manager will be responsible for coordinating and communicating all expectations both internally and with DHHR and is ultimately responsible for ensuring the project is completed on budget and on schedule.

Task Group	Task ID	WBS Control Number	Project Deliverables	Timeline In Days	Tellus Resource
1	D001	1.1	Project Kickoff Meeting	6	Project Manager
1	D002	1.2	Change Management Plan	20	Project Manager
1	D003	1.3	Communication Management Plan	20	Project Manager
1	D004	1.4	Cost Management Plan	20	Project Manager
1	D005	1.5	Document Management Plan	20	Business Analyst
1	D006	1.6	Modularity and Reusability Plan	24	Solution Architect
1	D007	1.7	Project Work Plan	24	Project Manager
1	D008	1.8	Quality Management Plan	24	QA Manager
1	D009	1.9	Risk & Issue Management Plan	24	QA Manager
1	D010	1.10	Schedule Management Plan	30	Project Manager
1	D011	1.11	Scope Management Plan	30	Project Manager
1	D012	1.12	Staffing Management Plan	30	Project Manager
1	D013	1.13	Stakeholder Management Plan & Analysis	31	Project Manager
2	D014	2.1	Data Management Plan	27	Solution Architect

2	D015	2.2	Data Security, Privacy & Confidentiality Plan	27	Solution Architect
2	D016	2.3	Incident Management Plan	27	QA Manager
2	D017	2.4	Master Test Plan	34	QA Manager
2	D018	2.5	Privacy Impact Analysis	30	Solution Architect
2	D019	2.6	Requirements Gap Analysis	30	Business Analyst
2	D020	2.7	Requirements Management Plan	30	Business Analyst
2	D021	2.8	Requirements Specification Document	44	Business Analyst
2	D022	2.9	Requirements Traceability Matrix	28	Business Analyst
2	D023	2.10	Safeguard Procedures Report	28	Report Developer
2	D024	2.11	Security Plan	28	Solution Architect
2	D025	2.12	System Backup and Record Retention Plan	28	Solution Architect
2	D026	2.13	System Requirement Document/User Stories	43	Business Analyst
3	D027	3.1	Capacity Plan	38	AWS Architect
3	D028	3.2	Configuration Management Plan	38	Solution Architect
3	D029	3.3	Data Conversion Plan	45	Integration Architect
3	D030	3.4	Data Conversion Test Cases	52	Integration Architect

3	D031	3.5	Data Conversion Test Results	76	Integration Architect
3	D032	3.6	Database Design Document & Data Models	38	AWS Architect
3	D033	3.7	Detailed System Design Document	38	Business Analyst
3	D034	3.8	Disaster Recovery & Business Continuity Plan	38	Solution Architect
3	D035	3.9	Federal Certification & Review Management Plan	64	Solution Architect
3	D036	3.10	Interface Inventory	94	Integration Architect
3	D037	3.11	Load & Stress Test Cases	91	Integration Architect
3	D038	3.12	Load & Stress Test Results	104	Integration Architect
3	D039	3.13	Operational Readiness Plan	104	Project Manager
3	D040	3.14	Operational Readiness Test Scripts	104	QA Manager
3	D041	3.15	Operational Readiness Test Results	105	Project Manager
3	D042	3.16	Regression Test Cases	99	QA Manager
3	D043	3.17	Regression Test Results	119	QA Manager
3	D044	3.18	Reports & Forms Inventory	93	Report Developer
3	D045	3.19	System Integration Plan	99	Integration Architect
3	D046	3.20	System Integration Test Cases	99	QA Manager

3	D047	3.21	System Integration Test Results	104	QA Manager
3	D048	3.22	Training Management Plan	122	Trainer
3	D049	3.23	User Acceptance Test Cases	105	QA Manager
3	D050	3.24	UAT Results & Letter of Completion	140	QA Manager
4	D051	4.1	Cutover Play Book	142	Project Manager
4	D052	4.2	Federal Review Supporting Documentation	146	Project Manager
4	D053	4.3	Implementation Certification Letter	146	Project Manager
4	D054	4.4	Implementation Plan	104	Project Manager
4	D055	4.5	Operations Change Management Plan	160	Project Manager
4	D056	4.6	Operational Milestone Review	155	Project Manager
4	D057	4.7	Production Screenshots, Reports & Data to Certify	155	Project Manager
4	D058	4.8	Report Distribution Schedule	169	Report Developer
4	D059	4.9	Solution Health Monitoring Plan	162	Business Analyst
4	D060	4.10	System Operations Plan	176	Solution Architect
4	D061	4.11	System & User Documentation	183	Business Analyst
4	D062	4.12	Training Materials	183	Trainer
4	D063	4.13	Training Report	183	Trainer

4	D064	4.14	Training Schedule	183	Trainer
4	D065	4.15	Turnover & Closeout Management Plan	183	Project Manager
5	D066	5.1	Project Schedule	171	Project Manager
5	D067	5.2	Project Status Reporting	171	Report Developer
5	D068	5.3	Risk Register/Exception Plan	171	QA Manager
5	D069	5.4	Updated Project Management Components	171	Project Manager
5	D070	5.5	Updated Requirements Traceability Matrix	190	Business Analyst
5	D071	5.6	Updated Training Management Plan	190	Trainer

The following table estimates the number of Tellus personnel hours required to complete the deliverables for each project phase including the resource named about and those supporting the lead Tellus Resource. Estimated hours are difficult to estimate in advance of solution planning so the following table may not be representative of actual time spent by resource to complete the required deliverables for each phase. Tellus is unable to estimate the number of hours required by DHHR personnel; however, we will strive to impact DHHR resources as minimally as possible to deliver a successful EVV Solution to DHHR.

Task Group	Phase	Resource	Hours
1	Project Initiation & Management Plan	AWS Architect	40
1	Project Initiation & Management Plan	Business Analyst	60
1	Project Initiation & Management Plan	Integration Architect	60
1	Project Initiation & Management Plan	Project Manager	270
1	Project Initiation & Management Plan	QA Manager	60
1	Project Initiation & Management Plan	Report Developer	0
1	Project Initiation & Management Plan	Solution Architect	40
1	Project Initiation & Management Plan	Trainer	40
2	Solution Planning	AWS Architect	60
2	Solution Planning	Business Analyst	400
2	Solution Planning	Integration Architect	200
2	Solution Planning	Project Manager	80
2	Solution Planning	QA Manager	40
2	Solution Planning	Report Developer	100
2	Solution Planning	Solution Architect	400
2	Solution Planning	Trainer	40
3	Solution Design, Test & Operational Readiness	AWS Architect	120
3	Solution Design, Test & Operational Readiness	Business Analyst	450
3	Solution Design, Test & Operational Readiness	Integration Architect	500
3	Solution Design, Test & Operational Readiness	Project Manager	40
3	Solution Design, Test & Operational Readiness	QA Manager	600
3	Solution Design, Test & Operational Readiness	Report Developer	200

3	Solution Design, Test & Operational Readiness	Solution Architect	800
3	Solution Design, Test & Operational Readiness	Trainer	800
4	Solution Deployment	AWS Architect	50
4	Solution Deployment	Business Analyst	400
4	Solution Deployment	Integration Architect	700
4	Solution Deployment	Project Manager	490
4	Solution Deployment	QA Manager	500
4	Solution Deployment	Report Developer	120
4	Solution Deployment	Solution Architect	200
4	Solution Deployment	Trainer	900
5	Project Monitor & Control	AWS Architect	20
5	Project Monitor & Control	Business Analyst	70
5	Project Monitor & Control	Integration Architect	40
5	Project Monitor & Control	Project Manager	140
5	Project Monitor & Control	QA Manager	140
5	Project Monitor & Control	Report Developer	40
5	Project Monitor & Control	Solution Architect	100
5	Project Monitor & Control	Trainer	300

The Draft Project Schedule identifies critical dependencies in column 6, "Predecessors". The number in the column designates the ID of the line item the task is dependent on. For example, Task ID 4, "Contract Execution" is dependent on Task ID 3 "Contract Negotiation/Review Period".

2 WORK BREAKDOWN STRUCTURE (WBS)

Our detailed West Virginia Draft Work Breakdown Structure is contained in this response as Addendum B.

The WBS is a hierarchical diagram directly associated to the Draft Project Schedule broken into Project Task Groups and Deliverables as outline in Section 4.6 of the RFP document.

The Draft WBS in conjunction with Draft Project Schedule and the tables presented in this attachment provide a full overview of our initial work plan. This plan is subject to change based on additional information that may be obtained through the contracting period and during the project initiation and solution planning phases of the engagement.

ATTACHMENT 6: MANDATORY REQUIREMENTS

Instructions: 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. 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). 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. See the attached Microsoft Excel® file titled, Attachment 6: Mandatory Requirements.

PROGRAM MANAGEMENT

MR001	1	All provided services must comply with the Department rules.

Tellus agrees to comply with all rules established by DHHR.

PROJECT MANAGEMENT

MR002	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).

Tellus agrees to adhere to the performance measures and penalties outlined within the service level agreements (SLAs) included in the request for proposal (RFP).

HARDWARE AND INFRASTRUCTURE

MR003	1	The Vendor must ensure that solution modules and applications integrate successfully and effectively with minimal or no customization.

Tellus supports the open/hybrid EVV model and publishes standard open Application Program Interfaces (APIs) promoting interoperability across the Medicaid ecosystem by integrating with care management applications, third-party EVV vendors and Medicaid Management Information Systems (MMIS).

Tellus has successfully and effectively integrated with both third-party EVV vendors and MMIS to capture and verify data with no customization thereby facilitating operational efficiency and workflow management while improving the accuracy of billing and payment structures for participating programs and services.

Bi-directional interfaces are written to integrate with a wide range of applications successfully and effectively with minimal customization. The following interchange protocols are supported by our modular integration engine:

- TCP/MLLP
- File (local file system and network shares)
- PDF and RTF documents
- JMS
- FTP/SFTP
- HTTP/Web Services
- SMTP
- SOAP (over HTTPS)
- DICOM
- JavaScript

Our open architecture also allows for the easy addition of custom and legacy interfaces.

Typical messaging standards supported by the Tellus data interchange solution include:

- Proprietary Layouts
- ANSI X.12 Electronic Data Interchange (EDI) including **834, 837I & 837P**
- HL7 (Health Level Seven) version 2 messages
- CDA (Clinical Data Architecture)/CDD (Continuity of Care Document)
- CSV (comma-separated variable)
- DICOM
- XML
- JSON
- NCPDP
- RAW
- JavaScript Batch
- Additional Data Types are support via API Libraries

Our flexible open architecture also allows custom and legacy interfaces to be easily added to support data sharing with systems that are not able to share information in one of our native protocols outlined above.

In addition to the ability to share data employing a wide variety of standards and protocols, data transfers can be set up to occur both near real-time or scheduled periodically as individual or batch transactions.

VISIT VERIFICATION

MR004	1	The solution must securely capture and electronically verify:
MR005	2	The identity of the member receiving services
MR006	2	The identity of the direct care worker making the visit
MR007	2	The identity of the provider agency
MR008	2	The date the visit begins and ends
MR009	2	The time the visit begins and ends
MR010	2	The location of the visit

MR011	2	The services being delivered
MR012	2	The waiver program or plan name

Tellus is fully compliant with the 21st Century Cures Act mandate capturing the following required data points for home and community-based personal and home health care services provided through a Medicaid state or waiver plan:

- Member receiving service
- Direct care worker providing service
- Start and End date of service
- Start and End time of service
- Location of service
- Type of services delivered

In addition, Tellus EVV natively captures the additional data points required by DHHR:

- Identity of provider agency
- Waiver program or plan name

Our EVV solution securely captures and stores each of these data points electronically.

SECURITY MANAGEMENT I

MR013	1	The solution must uniquely identify each user.

Access to our EVV solution is tightly controlled and monitored using a unique secure login ID and device access controls associated with each user. System security is integrated into the basic design of the application. Tellus employs layers of standard security features to make sure only authorized users can access the system and its data, including user authentication through IDs and passwords, functional access controls, multiple firewalls and complementary virus protection products. Data transmitted between external systems and our servers is protected by authentication and encryption, while secure file transfer

protocols (SFTP) are always used for data file transmissions.

The EVV mobile app is easily loaded onto devices used to capture EVV data by downloading the app from commercially available app stores onto any smart Android or iOS device meeting minimum requirements. The device is associated with the user by entering unique, valid login credentials including a login ID and password. A user cannot access member data unless they are associated with the member by an administrator at a provider agency or fiscal intermediary. The criteria to create multiple layers of authentication will include:

- User must be created with secure login credentials providing a unique identifier, either a cell phone or email address.
- User must be associated with a member by an administrator associated with a provider or fiscal intermediary.

Access to components of the application and the ability to view and write to specific fields is controlled by secure, private login credentials in conjunction with role-based permissions. User roles and associated permissions are defined during the solution planning phase of the project.

DATA SOURCES, DELIVERY, AND DISPLAY

MR014	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).

Tellus understands data sources will be identified based on the specifications and requirements of the RFP with collaboration between DHHR, MMIS Vendor and EVV Vendor. The team will work together to define the required source systems, data files, data elements, file transfer protocols and file interface definitions.

DHHR envisions the EVV Environment as depicted below:

The primary data sources for the EVV solution are expected to be MMIS and third-party EVV Vendors. Data exchanges will include operational and performance data. Tellus EVV will accept and aggregate all EVV data.

Tellus has experience supporting statewide EVV programs and interfacing with both MMIS and third-party EVV Vendors. We welcome the opportunity to propose recommendations to DHHR to fulfill the specifications outlined in the EVV RFP as well as information shared during stakeholder meetings and solution planning including:

- Data field names
- Data specifications such as lengths and layouts
- File sharing formats
- Data transfer protocols
- Data aggregation
- Data standardization

We are confident in our ability to objectively share options and the pros and cons associated with specific choices. Once the team chooses which data sources to include and the file transfer protocols to incorporate into the program, Tellus will work with all partners to ensure program goals are successfully designed and implemented.

PROJECT MANAGEMENT

MR015	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).

Tellus works with a third-party vendor to certify that our mobile apps, portals, corporate web site, and all training materials are ADA 508 compliant, and provides a VPAT report for each.

SECURITY MANAGEMENT II

MR016	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)

Tellus executes a Business Associate Agreement (BAA) with each subcontractor as a matter of policy.

MR017	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.

Tellus agrees to enter into Business Associate Agreements (BAA) with data partners as directed by DHHR.

MR018	1	The Vendor must ensure that all data submitted to or collected by the solution will remain the property of the Department.

Tellus understands all data submitted to or collected by the EVV solution is the property of DHHR.

MR019	1	The Vendor must agree to abide by all the Department security and privacy policies to protect confidential and sensitive information.

Tellus will abide by all DHHR security and privacy policies to protect confidential and sensitive information.

MR020	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)

Tellus is a healthcare services technology company. Our solution is operational with a security model incorporating the protection of data including safeguarding protected health information (PHI) and personally identifiable information (PII).

Tellus certifies compliance with HIPAA regulations and requirements as described in 45 CFR Parts 160, 162 and 164 along with the updated ARRA and HITECH act provisions as well as all HIPAA requirements related to privacy, security, transaction code sets (where applicable) and medical provider enumeration.

Security and privacy are very important from the signing of the contract through system closeout and turnover. Tellus understands the importance of enforcing PHI and PII restrictions. Tellus synchronizes standards and regulations to support an industry comprehensive set of requirements. Tellus implements and manages solutions based on the synchronized standards, regulations and customer requirements. Tellus applies controls based on jurisdictional prudence. If a local standard or regulation is more stringent, then it takes precedence in our planning.

Tellus offers added protection through the experience of our team. While privacy, security and confidentiality are supported by best practices, they rely on implementation by individuals who must know, understand and comply with those regulations and best practices. Tellus requires every employee and contractor to successfully pass on first hire, and annually thereafter, HIPAA-centered Privacy and Security Training.

All PHI data is encrypted in transit and at rest when stored in a database or filesystem. Tellus uses Transparent Data Encryption (TDE). The process of retrieving visit verifications in compliance with HIPAA standards requires all communications (application <--> database, mobile app > server) happen over a secure HTTPS connection. Tellus ensures that PHI information is encrypted when transmitted and encrypted at rest by using SSL/TLS and database encryption. Our hosting provider has achieved a number of certifications including, but not limited to, SOC 1,2,3, FedRAMP, ISO 9001, HITECH, PCI DSS: (https://aws.amazon.com/compliance/).

MR021	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)

Tellus EVV is compliant with a wide range of security and health information policies and protocols, including, but not limited to HIPAA, FIPS, NIST cryptographic standards, FedRAMP, ISO 9001, and HITECH. Tellus adheres to FIPS Pub 140-2 validated encryption as our minimum encryption standard.

CMS CERTIFICATION

MR022	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)

Tellus routinely monitors Centers for Medicare & Medicaid Services (CMS) communications and will remain in alignment with all future updates.

CMS recently published Medicaid Enterprise Certification Toolkit Version 2.3 (MECT v2.3) that applies to all MMIS and related state technology solutions excluding EVV. EVV requires a streamlined, outcomes-based approach to achieve certification. This approach focuses on demonstrating alignment with specific business outcomes. EVV certification is structured around the following elements:

- Pre Go-Live Operational Readiness Review
- Post Go-Live Certification Review (six months or more after Go-Live)
- Outcome statements
- Evaluation criteria and required evidence corresponding to outcome statements to evaluate the system's functionality and compliance with laws, regulations, and industry good practices
- Key performance indicators (KPIs) reported quarterly to support the outcome statements and track performance of the system over time

Tellus welcomes the opportunity to support DHHR in the CMS certification process.

MR023	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.

Tellus' software application architecture and processes support MITA goals and will support DHHR with MITA Self-Assessment and other MITA artifacts requested.

TELLUS EVV COMPLIES WITH THE SEVEN STANDARDS AND CONDITIONS ADVOCATED BY CMS AS FOLLOWS:

1	**Modularity Standard:** Tellus EVV is comprised of five (5) major modules, or components, that operate together or individually. The modules work seamlessly together in a runtime environment employing loosely coupled services. Real time rendered service data is available for claims pre-adjudication and 837 submission to MMIS on the day services are completed. Payer adjudication data can be imported to EVV and made available to providers as soon as the payer transmits the information to Tellus. Tellus can accept standard 835 or proprietary data formats.
2	**MITA Condition:** Tellus will assist the WDH in documenting "As-Is" and "To-Be" environments of business, information and technical capabilities demonstrating an increasing MITA maturity level, complying with MITA 3.0. Tellus will also strive to identify and recommend opportunities to leverage the reuse of healthcare technologies within the State and among states.
3	**Industry Standards Condition:** Tellus EVV is fully compliant with the following standards: a. Health Insurance Portability Act of 1996 (HIPAA) b. Health Information Technology for Economic and Clinical Health Act (HITECH) c. National Institute of Standards and Technology (NIST) Special Publication (SP) 800 d. Section 508 of the Rehabilitation Act, Americans with Disabilities Act (ADA) e. Federal Civil Rights Laws f. Section 1104 of the Affordable Care Act g. Section 1561 of the Affordable Care Act h. 45 CFR 164.316 and Administrative Rule 37.85.414

4	**Leverage Condition:** Tellus supports the open/hybrid EVV model and publishes standard open Application Program Interfaces (APIs) that promotes interoperability across the Medicaid ecosystem integrating with care management applications, third-party EVV vendors and MMIS.
5	**Business Rules Condition:** Tellus is passionate about understanding the perspectives of EVV constituents including payers, providers, participants and other interested parties. Our communications, outreach, training and customer support initiatives strive to promote a community of reliability, trust and respect. Our EVV solution supports accurate claims processing processes and procedures.
6	**Reporting Condition:** Tellus EVV collects and evaluates all the data necessary to evaluate the operation and performance of the EVV program to monitor and improve operations, transparency and accountability. AWS CloudWatch is used to monitor network traffic, bandwidth utilization and identify bottlenecks that impede performance. Monitoring and auto-scaling systems provide the information required to diagnose system performance issues, errors and backlogs. Monitoring includes, but is not limited to, CPU, memory utilization, network and disk utilization. For the database server we also monitor read/write latency, number of sessions, and session performance. Our engineers get immediate notifications regarding all system issues. If they cannot be resolved immediately, notifications will be forwarded to the WDH and/or Providers as required based on service level agreements.
7	**Interoperability Condition:** Tellus uses NextGen Connect (formerly Mirth Connect), an open source, cross-platform, bi-directional health care integration engine providing maximum flexibility to integrate with health information exchanges, public health agencies, human service programs and other community organizations as required.

Tellus is committed to developing CMS compliant solutions and will continue to monitor CMS guidelines to ensure our product roadmap is aligned with their objectives

MR024	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)

Tellus will work with DHHR to coordinate and develop all documentation requested by CMS to achieve certification in accordance with the most recent MECT, as required. Currently EVV is excluded from the provisions outlined in MECT v2.3 and instead is subject to EVV Certification Version 1.0.

TELLUS WILL DEVELOP AND SUPPORT DOCUMENTATION TO ACHIEVE CERTIFICATION BASED ON THE FOLLOWING CMS OUTCOMES, CRITERIA, EVIDENCE AND KPIS:

EVV OUTCOME 1	EVV Solution enhances the ability to detect fraud, waste, and abuse through increased visibility into its Home and Community-based Services Programs (EVV Criteria 1 – 6)
EVV OUTCOME 1 KPIs:	1. Association of EVV record to claim/encounter. **Calculation** Claims and encounters counted in this calculation are those that are non-duplicative and were paid during the quarter. $\% = \frac{\text{\# of paid claims and encounters that have complete EVV visit records associated with them}}{\text{\# of paid claims and encounters for PCS and/or HHCS}} \times 100$ 2. EVV record match against approved services, providers and units

Calculation
Claims/encounter procedure codes counted in this calculation are those that are non-duplicative and were paid during the quarter.

$$\% = \frac{\text{\# of procedure codes paid for which units, provider, and service were approved / authorized}}{\text{\# of home visit procedure codes paid}} \times 100$$

3. EVV records without manual edits
Calculation
EVV records counted in this calculation are those that are non-duplicative and were received during the quarter.

$$\% = \frac{\text{\# of EVV records for verified visits which have no manual edits}}{\text{\# of EVV records for verified visits received}} \times 100$$

EVV1 CRITERIA	The electronic visit verification (EVV) solution captures and verifies data with respect to personal care services or home healthcare services, including: • Type of service performed; • Individual receiving the service; • Date of service; • Location of service delivery; • Individual providing the service; and Time the service begins and ends.
EVV1 Evidence	1.1: Automated test report and screenshot(s) verifying that the EVV solution captures service type.

	1.2: Automated test report and screenshot(s) verifying that the EVV solution captures service location. 1.3: Automated test report and screenshot(s) verifying that the EVV solution captures which individual provided the service and which individual received the service. 1.4: Automated test report and screenshot(s) verifying that the EVV solution correctly captures the beginning and end time of service visit. 1.5: Automated test report and screenshot(s) verifying that the EVV solution correctly and completely 1) stores and 2) transmits all required data elements to the state's chosen database. For the certification review, state needs to provide evidence showing that these six data elements were being collected as far back as the date from which the state is requesting enhanced funding. 1.6: Automated test report and screenshot(s) verifying that users can retrieve records by searching on one or more of the individual elements (i.e., service type, date, individual, date, etc.) 1.7: Automated test report and screenshot(s) verifying that the EVV solution identifies incomplete records.
EVV2 Criteria	For states that mandate or offer the use of a state procured EVV solution, the EVV solution is able to save and transmit data regardless of the mode of communication (for example, network connectivity, telephony, cell coverage). The system is designed such that even if there is a break in communication service, the data is stored and can be transmitted when service is restored.
EVV2 Evidence	2.1: Explanation of how the solution (primary and alternate taken together) can store and transmit data in cases where the communication service is interrupted. Include relevant screenshots (such as timestamp logs showing the delay between the time the visit ended and was logged and when the data was received.)

EVV3 Criteria	Each visit initiated is captured within the EVV system, whether or not the visit was verified.
EVV3 Evidence	3.1: Automated test report and screenshot verifying that EVV visit information is captured, even if the visit is not verified by the beneficiary or a caregiver.
EVV4 Criteria	For states that receive EVV data from various EVV platforms, the state standardizes EVV data elements. The state validates incoming data against its EVV data standards. (This could be through the EVV solution or through some other data aggregation function.)
EVV4 Evidence	4.1: Automated test report and screenshot showing that data elements received by the EVV solution or data aggregator that are not compliant with the state's EVV data definitions are rejected and that the system returns an error message to the sender. 4.2: Automated test report and screenshot showing that data elements received by the EVV solution or data aggregator that are compliant with the state's EVV data definitions are accepted. 4.3: The state's EVV data definitions, available to all relevant stakeholders.
EVV5 Criteria	The state Medicaid agency uses the EVV data to avoid paying for unauthorized or unapproved services. The state uses EVV data to check that for each claim/encounter, 1) the provider in the EVV visit record is approved for the beneficiary and matches the one in the claim / encounter submission, 2) the visit procedure codes match those in the EVV record, 3) the visit procedure codes in the record are approved for the beneficiary, and

	4) the number of units charged for a beneficiary does not exceed the beneficiary's total number of approved units. Validations need not be part of the EVV system; they can be done as part of claims adjudication or another function. This criterion applies to benefits given under all relevant authorizations. Approval could be in the form of a physician's order, prior authorization, service plan, or other forms of approvals under relevant authorities.
EVV5 Evidence	5.1: Explanation of 1) how the state uses EVV data to check each of the items listed for encounters, if applicable, and 2) how the state uses EVV data to apply edits to claims. 5.2: Screenshots showing claims that were edited along with reason codes for the following scenarios: • Provider mismatch • Type of services not approved for that beneficiary • Number of units not approved or that exceed an approved amount
EVV6 Criteria	All EVV data flows and interfaces are documented and tested, such as data flow from state-provided devices / telephony, non-state run EVV platforms and data aggregator, and to other Medicaid systems.
EVV6 Evidence	6.1: Automated test report(s) and screenshot(s) verifying that the EVV solution correctly transfers and receives data to/from all interfacing systems and that incorrect transmissions are flagged, and error messages are generated. 6.2: High level diagram showing all interfaces and types of data flow. 6.3: Explanation of how changes to the system is communicated to stakeholders.

	If this is automated, example informational message.

EVV OUTCOME 2	EVV Solution is reliable, accessible and minimally burdensome on providers, beneficiaries, and their caregivers (EVV Criteria 7 – 10)
EVV OUTCOME 2 KPIs:	Ensure EVV system has high availability. **Calculation** During the second quarter having two 30-day months and one 31-day month, there were three, five-hour scheduled maintenance windows. The EVV solution application was unavailable for 121 minutes outside of this window. Minutes in the quarter = (2 x 30 days x 24 hours x 60 minutes) + (31 days x 24 hours x 60 minutes) = 86,400 + 44,640 = 131,040 Minutes of scheduled maintenance = 15 hours x 60 minutes = 900 Minutes in month not including scheduled maintenance (time the EVV solution should have been up) = 131,040 – 900 = 130,140 Uptime = 130,140– 121 = 130,019 The performance therefore = 100 x (130,019) ÷ (130,140) = 99.9%

EVV7 CRITERIA	For states that mandate or offer the use of a state procured EVV solution, providers, beneficiaries, and caregivers are able to submit the necessary verification information via alternate methods, should the primary mode of submission be out of service. (For example, if a handheld device is not working properly, the provider is able to phone in the visit information or submit it via a website portal.)
EVV7 EVIDENCE	7.1: Automated test report and screenshot(s) showing that, for each alternative submission method, the required EVV data is correctly received and stored. 7.2: Training materials for users that explain how visit information can be submitted should the primary method of submission be out of service.
EVV8 CRITERIA	For states that mandate or offer the use of a state procured EVV solution, the system must be accessible for individuals with physical disabilities and vision impairments and satisfy the requirements of the Americans with Disabilities Act of 1990, Section 504 of the Rehabilitation Act of 1973, 36 CFR Part 1194, 42 CFR 431.206, and 45 CFR Part 80.
EVV8 Evidence	8.1: Detailed 508 test report.
EVV9 CRITERIA	The state provides user training and stakeholder outreach.
EVV9	9.1: Training plan and materials, record of when trainings occurred or are

EVIDENCE	scheduled, and for which stakeholder groups. For states that only aggregate data from providers' or MCOs' EVV platforms, this means an explanation of how those stakeholders can properly send data to the state.

EVV OUTCOME 3	EVV Solution ensures appropriate safeguards of electronic protected health information and personally identifiable information are implemented and maintained (Security1)
EVV OUTCOME 3 KPIs:	Ensure state is managing privacy and security risks. **Calculation** Number of known, unmitigated vulnerabilities in high or very high-risk levels. This number is determined by an independent third-party security and privacy auditor. Auditors must use the risk assessment scale as defined in NIST SP 800-30, Revision 1 (see Figure 1 below). The first reporting of this metric should be based on an independent, third-party audit, but follow-on reporting of this KPI can be based on the state's own periodic risk assessment (should be at least annually or when there are significant changes to the system). If CMS changes their EVV certification criteria, Tellus will revise certification documentation according to any and all revised guidelines.
SECURITY 1 CRITERIA	The solution, employees, contractors, and downstream subcontractors or entities that create, collect, disclose, access, maintain, store, and use

	electronic PHI/PII must comply with the HIPAA privacy, security, and breach notification regulations, and applicable state and federal laws and regulations.
SECURITY 1 EVIDENCE	S1.1: A recent penetration test report and security and privacy controls assessment report (SAR). A penetration test must accompany a SAR to ensure the effectiveness of its baseline controls implementation (NIST SP 800-171 tailored controls or NIST SP 800-53 tailored controls). S1.2: Independent, third-party security and privacy controls assessment report that covers compliance with 1) NIST SP 800-171 and/or NIST SP 800-53 standards and all relevant controls in HIPAA; 2) aligning Health Care Industry Security Approaches pursuant to Cybersecurity Act of 2015, Section 405(d), and 3) the Open Web Application Security Project Top 10. Risks should be identified using NIST SP 800-30 Revision 1. The third-party audit should include, but need not be limited to, a penetration test, a review of all HIPPA compliance areas: user authentication; information disclosure; audit trail; data transfers; and information on correct data use (role-based testing of use). The audit should cover adequate audit trails and logs (ID, access level, action performed, etc.). Audit should also cover encryption of data at rest, in audit logs, and in transit between workstations and mobile devices (where applicable), to external locations and to offline storage.

ATTACHMENT 7: BUSINESS SPECIFICATIONS APPROACH

Instructions: 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. 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 specifications included in RFP Section 4: Project Specifications. 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. 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.

1.1 VISIT VERIFICATION

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.

Tellus EVV is a SaaS-based application built from the ground up to provide maximum flexibility with minimal effort. Configuration settings, variable parameters and business rules that are separate from our code base provide the ability to deploy a highly flexible and adaptable solution for any environment very quickly. This includes the ability to manage multiple programs with different rules and edits.

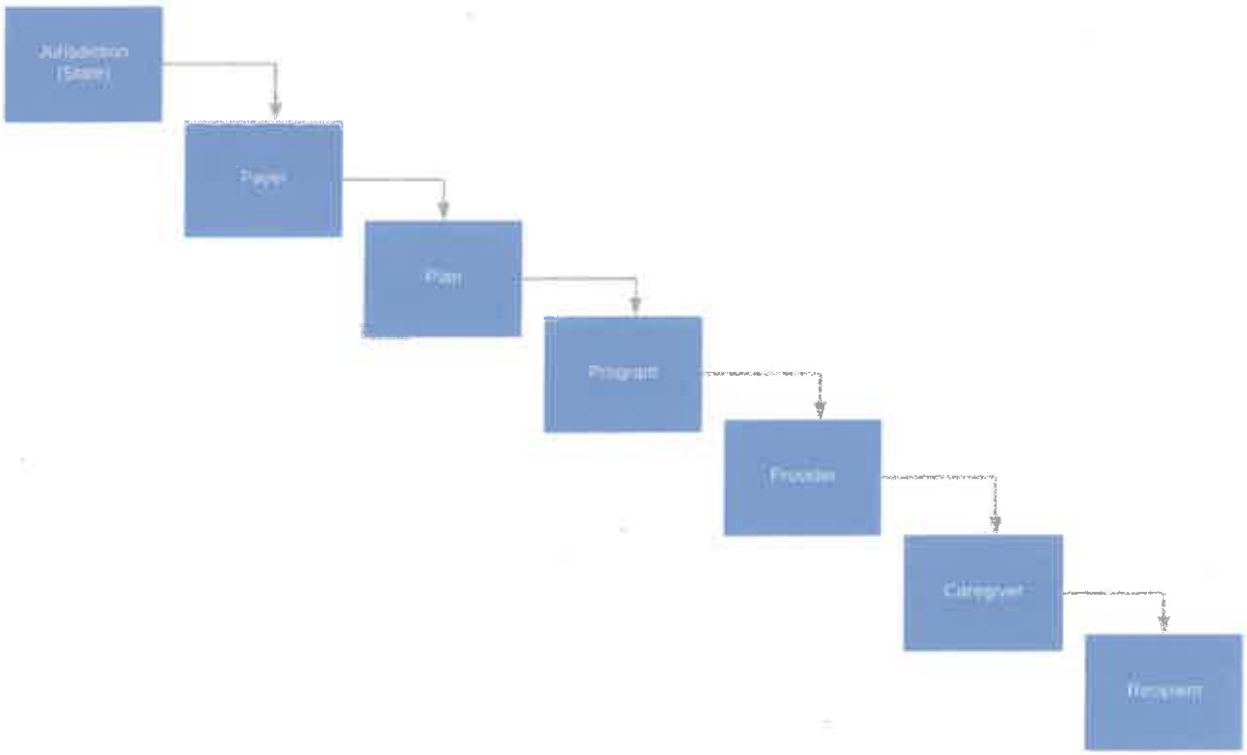
Business rules are written and enforced based on the following hierarchy and can be written at any level:

Rule Hierarchy Level	Example
Jurisdiction	West Virginia

Payer	WV Medicaid, Managed Care Organization (MCO)
Plan	Home & Community Based Services, Behavior Analysis
Program	Aged & Disabled Waiver, Traumatic Brain Injury Waiver
Provider	Traditional Agency Model, Fiscal Employer Agent
Caregiver	Direct Care Worker, Personal Attendant
Member	Individual Member, Designated Representative

This classification system enables DHHR to configure the EVV application business rules at any level in the hierarchy. Program rules, services, policies and procedures and reimbursement rates can be defined at the program and even the provider level. Our business intelligence rules engine is a module independent of the software code base, as a result, rules can be easily configured during the implementation period and changed during the term of the contract without the use of development resources, providing maximum flexibility.

The following diagram depicts the native rule hierarchy Tellus EVV is architected to support:



The highest level in the rule hierarchy, Jurisdiction, applies to all levels within the organization. If DHHR establishes a rule such as all EVV data must be aggregated, that rule applies to every payer, plan, program, provider, caregiver and member receiving care requiring EVV.

If DHHR determines that for the Traumatic Brain Injury Waiver (TBIW) program a late visit as one that starts more than fifteen (15) minutes after the scheduled visit time, that rule applies to all providers, caregivers and members receiving care under the TBIW program. All visits related to the TBIW program that start more than fifteen (15) minutes after the scheduled visit time will be flagged as late in the EVV database and will be reflected as such in at all points in the application and for reporting purposes.

User-based permissions provide the additional benefit of customizing user privileges at any of the levels in the hierarchy including by program. That means a provider can be granted

the right to enter service tasks on one program by personnel type and not have that same access for another program.

Service task lists can vary and be customized based on program needs and rules. Another configurable option is to allow or disallow direct care workers to enter notes and/or alerts using their mobile device. This option provides the ability for the direct care worker to effectively and efficiently communicate member status to provider administrators, fiscal employer agents and/or case managers.

Tellus EVV is flexible and adaptable to meet the needs of DHHR, your members and constituents.

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:
VV003	5075	2	Individual receiving services
VV004	5076	2	Direct care worker
VV005	5077	2	Billing provider agency
VV006	5079	2	Location of visit
VV007	5080	2	Date of visit
VV008	5081	2	Visit start time
VV009	5082	2	Visit finish time
VV010	5083	2	Missed visits
VV011	5084	2	Late visits
VV012	5085	2	Services delivered, including billing code and modifiers
VV013	5086	2	Independent verification by individual receiving services

VV014	5087	2	Payer
VV015	5088	2	Manual or electronic verification
VV016	5089	2	Data collection system, including the Department solution and other approved third-party electronic visit verification (EVV) systems

Tellus EVV is operational and electronically captures all the data elements outlined in the detailed specifications referenced above. Some of these data elements are required by the 21st Century Cures Act, others are natively built into the core functionality of our EVV solution and several will be derived based on the specific requirements for DHHR's EVV program implementation.

Tellus is fully compliant with the 21st Century Cures Act mandate capturing the following required data points for home and community-based personal and home health care services provided through a Medicaid state or waiver plan:

- Individual receiving service
- Direct care worker providing service
- Date of service
- Visit start time
- Visit end time
- Location of visit
- Services delivered

In addition, Tellus EVV natively captures the following additional data points required by DHHR:

- Billing provider agency
- Independent verification by individual receiving services
- Payer
- Manual or electronic verification

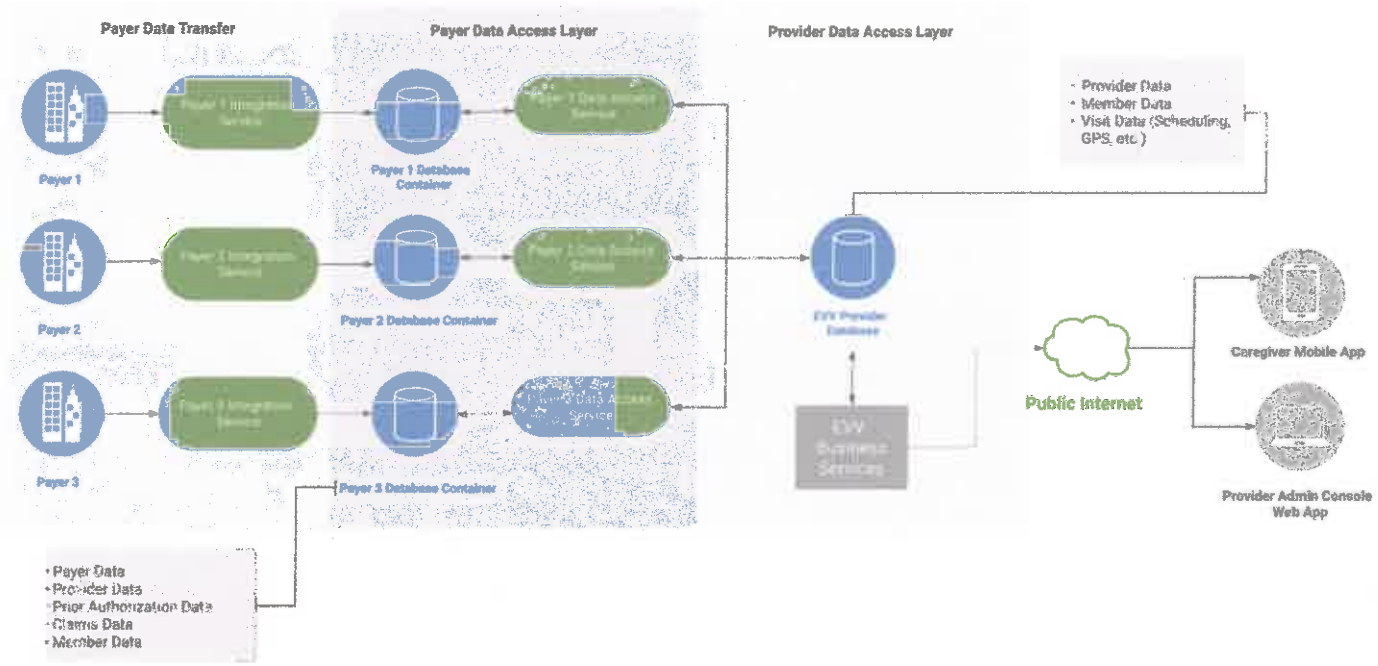
During the solution planning phase Tellus will collaborate with DHHR and MMIS to define the criteria related to the remaining data points referenced in the detailed specifications:

- Missed visits – DHHR will define the parameters for a missed visit. For example, the rule may state, if a visit is scheduled for February 15th and the direct care worker has not started the visit by midnight of February 16th, the visit is labeled "Missed".
- Late visits – DHHR will define the parameters for a late visit. For example, the rule may state, if a visit is not started by the direct care worker within one (1) hour of the scheduled visit time, the visit is labeled "Late".
- Service billing codes and modifiers – DHHR and MMIS will define and provide service billing codes, modifiers and associated rules the EVV solution will monitor and the data sharing mechanisms that will be employed to integrate information related to services approved for specific members on a continuous basis to verify visits and submit claims.
- EVV data collected and aggregated will retain the original data source and whether it was captured by the DHHR selected EVV solution or a 3rd party vendor, including the identity of the vendor.

All data is captured electronically and available for monthly and ad hoc reporting.

VV017	4220	1	The solution should have the ability to integrate the scheduling, authorization monitoring, visit verification, and billing.

Tellus EVV is a fully integrated solution incorporating scheduling, authorization monitoring, visit verification and billing. The following diagram depicts a high-level overview of the most common data flow supporting the ability to accurately schedule, monitor authorizations, verify visits and submit claims for eligible Medicaid Members:



Payer Data Transfer

Payers share the following data with Tellus:

Participating Providers,
Eligible Members,
EVV Billing Codes with related Modifiers,
Prior Authorized Services (PA) for each Member,
Active Direct Care Workers (if applicable).

Payer Data Access Layer

Payer data is imported into the Tellus EVV solution. Data for each Payer is segregated into a siloed database. Data is imported as frequently as the Payer makes it available, up to near real time.

Provider Data Access Layer

Provider Administrators can access data as soon as it is loaded into the Payer database over the web using standard, commercially available personal computers and standard web browsers by logging into the Tellus EVV Administrator Console.

Providers can only access Members who are linked to them through the Prior Authorizations transmitted by the Payer or their designated Utilization Management Vendor. Once a Member is associated with the Provider through the PA, the Provider can access Member data and schedule visits for that Member. A visit is scheduled by selecting a Member, a service the Member is authorized to receive and the Direct Care Worker who will provide the service. The visit is scheduled for a specific date, time and location.

Once a visit is scheduled, the Direct Care Worker selected to provide the service will be able to access the scheduled visit on their mobile device.

When the Direct Care Worker arrives at the scheduled location, the visit is started on their mobile device. The start date, time and location coordinates are capture and compared to the scheduled visit date, time and location when the "Start" button is pushed. At the end of the visit, the Direct Care Worker checks off the services provided, gets Member confirmation the services were provided and then ends the visit. When the Direct Care Worker pushes the button to end the visit, the end date, time and location coordinates are captured and compared to the scheduled visit.

The duration of the visit is captured and converted into units corresponding to the billing code modifier combination associated with the services rendered. The visit information is compared to the PA for the Member who received the services. If the services rendered are valid based on the Member PA date range and remaining units available, the services are ready to be billed by the Provider Agency.

When the Provider Agency submits the claim, it is electronically transferred from Tellus EVV to MMIS for claims adjudication.

Electronic data sharing and integration improves efficiency and reduces the opportunity for error, fraud, waste and abuse.

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.

One of the core components of Tellus EVV is our business intelligence rules engine. DHHR will define EVV program requirements and Tellus will write or configure previously written rules to ensure DHHR rules are enforced. For example, if a Member is authorized to receive benefits under service code S5130 and the provider administrator begins to schedule a visit for that Member under service code S5131, DHHR may choose to:

- Warn the user they are scheduling a visit for an unauthorized service and allow the visit to be scheduled, or
- Prevent the user from scheduling the unauthorized service

Tellus will configure all program requirements according to DHHR guidelines.

User-facing interfaces include a full suite of business rules to support EVV program requirements as well as data validation checks to prevent data entry errors. For example, valid entries for gender may be defined as "M" or "F". If the user accidentally enters "N" in the gender field that entry will not be accepted, the user will be notified they are entering invalid data.

Because our business intelligence rules engine is a modular component and rules are not written in the application code, DHHR requirements can easily be accommodated during the implementation phase of the project and if necessary, they can modify during the contract period.

VV019	4182	1	The solution should securely capture an independent verification of the service delivery from the member receiving services.

Tellus EVV securely captures independent verification of service delivery from the member receiving services at the end of the visit. After services are rendered the caregiver ends the visit, and the date, time and location are electronically captured.

The member will then sign the screen on the mobile device capturing the visit information to confirm receipt of services. This confirmation is captured in the EVV database and can be

viewed by provider administrators by accessing the visit details on their web portal as well as for reporting and audit purposes.

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.

Tellus EVV captures visits to multiple participants on a given day by a single direct care worker or provider agency is the most frequently occurring pattern for visit activity and is supported by Tellus EVV.

Our EVV solution does not restrict the number of visits a direct care worker or provider agency can complete within a 24-hour period. A direct care worker cannot be scheduled or logged into more than one visit at the same time. Rules can be written at the payer of program level to restrict the number of hours a direct care worker is eligible to work within a 24-hour period if requested by DHHR.

VV021	4191	1	The solution should account for living arrangements in which multiple members receiving services reside at a single address.

Tellus EVV supports living arrangements in which services are rendered to more than one member at the same address. EVV captures the rendered service information. Member address of record is typically one of the components shared with Tellus EVV in the form of a member data feed. The member address of record is always retained and can only be over-written by a subsequent payer data feed. Provider agency administrators have the ability to enter additional addresses on the member record if services will be rendered at other locations. When scheduling a visit, the provider administrator selects the address location for the visit and the direct care worker starts the visit when they arrive at the scheduled address location. If the visit is started at the scheduled address, pre-adjudication rules acknowledge the scheduled address and rendered service address are the same. If the visit is started at an address that is not the scheduled address, pre-adjudication rules flag the visit and a reason code must be entered before the service can be submitted for claims processing.

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.

Tellus EVV supports multiple visits per day to one participant by multiple caregivers or providers is supported by Tellus EVV. EVV captures the rendered service information including which provider and direct care worker attended to the member, pre-adjudication rules run against that utilization management data including member eligibility, approved services and the delivery frequency for each service. If the completed visit data is consistent with the utilization management criteria, the provider will be able to submit the completed visits for claims adjudication. If it does not, the provider must explain the deviation(s) by adding reason codes before submitting the visit for claims adjudication. All changes and explanations are retained in an audit log available for review and reporting.

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.

Tellus EVV supports services provided to a group of participants during a single visit, consistent with State guidelines, policies and manuals, including any additions or updates thereto on group visits: EVV captures the rendered service information, pre-adjudication rules run against that data based on information provided at the payer and program level to determine whether or not the collected data meets claims submission criteria. If it does, the provider can submit the visit for claims adjudication. If it does not, the provider must explain why by adding reason codes before submitting the visit for claims adjudication. All changes and explanations are retained in an audit log and can be reviewed and reported. Typically, in these instances, there is a modifier associated with it or a type of residence indicator associated with the participant.

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.

Tellus EVV supports situations where services are provided to a member where the member and direct care worker reside at the same address. This situation most frequently occurs in the Self-Directed delivery model. Our EVV solution supports this staffing scenario as well as many other unique features of the self-directed delivery model.

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.

Tellus EVV accounts for situations in which a visit starts and/or ends away from the member's residence. The member's address of record is typically transmitted by the payer in the member data feed. This address populates on the member's EVV profile and cannot be changed unless it is updated in a subsequent data feed. If DHHR chooses to allow providers to schedule visits at locations other than the address of record, the provider can add those addresses to the member profile in Tellus EVV. Services can be scheduled at any address on the member record including community-based settings and temporary addresses.

If the member visit is started or ended at an address that is different than the scheduled visit start or end address, the provider will have to explain the reason for the difference prior to submitting the claim for adjudication.

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.

Tellus EVV is highly configurable and can either allow or prevent multiple direct care workers and/or provider agencies from providing services to a member at the same time. As an example, business rules managing the permission for more than one direct care worker or provider can be developed and applied based on the program the member is enrolled in or the service code and modifier combination of the scheduled visit.

EVV captures all data points related to the delivered service. Pre-adjudication rules compare that data to the scheduled visit and to payer and program level rules to determine whether the collected data meets claims submission criteria. Visit data is also compared to prior authorized services for the member. If completed visit information passes all the associated validation rules, the provider can submit the visit to the payer for claims adjudication. If it does not, the provider must explain the deviation by adding reason codes before submitting the visit for claims adjudication. All changes and explanations are retained in an audit log and can be reviewed and included in reporting.

VV027	4185	1	The solution should verify that the agency providing the service has a valid pre-authorization for each member served on file.

Tellus EVV employs data validation rules to match the agency providing the service to a member to the pre-authorization supplied by the Utilization Management Company. In our standard use case, DHHR will share a member data feed with our EVV platform. The Utilization Management Company will share prior authorizations with the EVV platform.

Each prior authorization is linked to a member and a provider agency. When the prior authorization is loaded, it links the member to a provider agency in EVV. This relationship is used by our business intelligence rules engine to verify the agency providing the service is approved to render services to the member.

Business intelligence rules can be written to prevent behavior and/or to warn users they may be violating rules that could result in non-payment for delivered services. Examples include the following:

Activity	Preventive Measure	Warning
Provider agency searches for a member, no PA has been issued for the member.	Agency cannot see any information for the member until a PA is issued for the agency to provide services to the member.	Agency can manually add the member to their portal.
Provider agency is scheduling a visit for a member outside of PA service date range.	Agency receives an error message and cannot schedule the visit until a PA is issued.	Agency can schedule the visit but is warned the member does not have a valid PA.
Provider agency is scheduling a visit for a member, there are no units remaining on the PA.	Agency receives an error message and cannot schedule the visit until the PA is modified or a new PA is issued.	Agency can schedule the visit but is warned the member does not have a valid PA.

If the provider agency is permitted to manually add members and/or schedule visits for members who do not have valid PA's loaded in EVV and the PA is never received, DHHR rules will dictate if the claim can be submitted for adjudication. DHHR may determine if a valid PA is not submitted to the EVV system, the visit is not eligible for payment and may not be submitted. Alternatively, DHHR may determine, a visit without a valid PA can be submitted for adjudication if the agency explains why the visit was completed in the absence of a valid PA.

If a valid PA is submitted to the EVV system after the member is manually added by the agency or after the visit is scheduled, the PA will be available to the business intelligence rules engine to match the completed visit to the PA data. Once matched, the visit is available to be submitted for adjudication in the normal course of business.

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.

Tellus EVV is constructed to verify the time of the visit. As explained in our response to VV027, our business intelligence rules engine compares the completed visit date and time

to the prior authorization. If the visit meets the specifications defined in the prior authorization, the visit will match and can be submitted for claims adjudication. If the completed visit data and time does not meet the specifications defined in the prior authorization, Tellus will design the workflow to meet the requirements outlined by DHHR in the solution planning phase of the engagement. The EVV solution can prevent the submission of claims if the parameters do not align or the solution can require the provider to enter an explanation for the deviation and then allow the claim to be submitted for adjudication.

The date and time format can be captured or converted to YYYY-MM-DDTHH:MM:SS or an equivalent format acceptable to DHHR.

VV029	4202	1	The solution should have the ability to allow the Department to identify circumstances in which visit verification is not necessary.

Tellus EVV business intelligence rules engine can differentiate between services that require electronic verification and those that do not. During the solution planning phase of the engagement, DHHR will define which program and service combinations require electronic verification and which do not. Tellus will either write new rules or configure existing rules to accommodate DHHR goals and objectives. Because our business intelligence rules engine is a modular component of our EVV solution, rules can easily be written or configured without impacting our standard code base. This provides maximum flexibility during implementation and rules can also be modified during the term of the contract.

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.

Tellus EVV Provider Dashboard provides near-real-time alerting on all late visits. Visits schedules are either entered or imported into the EVV database. Direct Care Workers and provider administrators can view their visit schedules at will. When the scheduled Direct

Care Worker arrives at the visit location, they start the visit on their mobile device. If the visit is not started on time, the provider administrator is notified the visit is late.

The following criteria will be defined by DHHR during the solution planning phase of the engagement and the related rules will be entered into the Tellus business intelligence rules engine during the implementation phase:

Criteria	Example
Definition of Late	Visit must be started within 15 minutes of scheduled time, Visit must be started anytime on the date it is scheduled
Who to Alert	Direct Care Worker, Provider Administrator, Case Manager
Method of Alert	Display Late Visit on Provider Administrator Dashboard, Send SMS text Message to Case Manager
Alert Cadence	If Visit is 15 minutes late, display on Provider Administrator Dashboard, if Visit is an hour late, escalate Alert to SMS text the Case Manager

VV031	4195	1	The solution should have the ability to account for circumstances in which a visit crosses calendar days.

Overnight visits crossing calendar days are supported by Tellus EVV without requiring the direct care worker to clock-in or clock-out more than one time each. Tellus EVV captures the rendered service data. Like other types of visits, pre-adjudication rules run against the data based on information provided at the payer and program level to determine whether the collected data meets claims submission criteria. If it does, it will be a matched claim, and the provider agency can submit the visit for claims adjudication. If it does not, the provider must remediate the visit and provide, at minimum, a reason code for the manual modification before submitting the visit for claims adjudication. All changes to visit data and explanations are retained in an audit log and can be reviewed and reported.

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.

Tellus EVV accommodates different definitions of pending, late and missed visits at the applicable program and/or waiver service. During the solution planning phase of the engagement, DHHR will define what each visit status means for each program and/or waiver service subject to EVV services. Tellus will implement these definitions using our business intelligence rules engine. Visit statuses display on the administrator console, examples include:

- Not Started = Scheduled Visit for a future Date/Time
- Not Started, Late = Scheduled Visit for later Today
- Completed = Visit Started and Completed On-Time
- Completed, Late = Visit Started Late and Completed
- In Progress = Visit Started On-Time and currently In Progress
- In Progress, Late = Visit Started Late and currently In Progress
- Missed = Visit Scheduled prior to today and Not Started
- Unable to Complete = Visit Scheduled, Direct Care Worker reports for duty but cannot render services

If a visit is recorded as "Unable to Complete" our standard business logic requires the direct care worker to select a reason they cannot render services. Examples include: member not home, member hospitalized, member refuses treatment. DHHR can request more or other Unable to Complete reason codes to electronically capture during the solution planning phase of the engagement.

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.

Reporting a possible problem related to a visit verification can be accommodated by Tellus EVV. Currently business rules accommodated the ability for direct caregivers to communicate with provider agencies by sending an SMS text that is viewable on the provider administrator dashboard near real time as a configurable option. Direct care

workers enter notes, problems and/or alerts using their mobile device to effectively and efficiently communicate member status to provider administrators and/or case managers.

Additional and/or alternative communication methods can be accommodated using our business intelligence rules engine. Tellus EVV is flexible and adaptable to the different business processes for each DHHR program.

1.2 PROGRAM MANAGEMENT

PG001	3994	1	The solution rules/procedures should allow and enforce multiple service limits for different service ranges including, but not limited to:
PG002	5140	2	Day
PG003	5141	2	Week
PG004	5142	2	Month
PG005	5143	2	Year

Tellus EVV supports utilization management service limits expressed by day, week, month, and year as well as other increments. Utilization management criteria will be defined by DHHR during the solution planning phase of the engagement. Business logic to support that criteria at the service code/modifier level will be written and/or configured using our business intelligence rules engine and implemented in the EVV solution prior to the testing phase of the engagement.

PG006	3995	1	The solution rules/procedures should accommodate retroactive prior authorizations and changes to prior authorizations based on revisions to members' plans of care/service plans.

Tellus EVV supports retroactive prior authorizations (PAs), and changes to existing PAs based on revisions to the members' plan(s) of care.

Typically, Tellus EVV receives PAs in an electronic data feed from the payor or their utilization management vendor. captures each of these data points electronically. Data fields include Member ID, Provider ID, Service Code, Modifier (if any), Number of Units Available, Start Date, End Date, Frequency. PA data is electronically transferred from the payer to Tellus.

If a provider is permitted to schedule and/or complete a visit for a member without a PA and the PA is retroactively received in a data feed, the PA will be loaded into the application. Matching algorithms run in the background every ten minutes comparing: scheduled services, rendered services, prior authorizations will associate the PA when it is received and the completed visit that was in an "Unmatched" status because the PA did not exist, will be "Matched" the next time the algorithm runs. Once "Matched" the visit can be submitted by the provider to MMIS for claims adjudication.

PG007	4001	1	The solution should have the ability to round service delivery time.

Tellus EVV supports a fully configurable approach to round service delivery time in two ways:

1. Conversion of PA units to time
2. Rounding the duration of service delivery time calculated by comparing start time to end time

As a default, visit duration rounds to the nearest minute. Service codes typically round to units with the rounding rule dependent upon the PA unit type. The table below summarizes examples of currently available configurable options:

PA Unit Type	Unit Duration	Visit Duration, Rounding Rule
Q	Quarter Hour	0 - 15 Minutes Less than/equal to 7 minutes = 0 Units Greater than 7 minutes = 1 Unit
H	Hour	0 - 60 (minutes) Less than/equal to 30 minutes = 0 Units Greater than 30 minutes = 1 Unit
V	Visit	Ignore Visit Duration Completed Visit = 1 Unit

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.

Tellus EVV creates a master client index, also known as a globally unique identifier (GUID) for all members. The unique identifier is created by concatenating key business data for each member, such as combining Medicaid ID and Date of Birth for a specific member to create an internal database GUID key. This means all member data received during the contract period will be related. So, if a member becomes eligible for services on December 1st the data imported from DHHR notifying Tellus of eligibility will be matched and associated with that member even if the last time they received services was June of the prior year.

PG009	4768	1	The solution should maintain an integrated repository of provider agency information, including a single unique identifier, for all providers.

Tellus EVV creates an integrated repository of provider agency information, including a unique identifier for all providers, also known as a globally unique identifier (GUID). The unique identifier is created by concatenating key business data for each provider such as EIN-NPI-NPI Zip Code.

PG010	3957	1	The solution should be able to capture, verify, and support billing for in-home and community-based setting service visits.

Tellus EVV captures, verifies and supports billing for in-home and community-based setting service visits. Our solution supports multiple data capture options at the point of care including GPS enabled mobile apps, integrated voice response (IVR) accessed using the member's landline, digital hardware tokens and web portal data entry in the event of unusual circumstances that require exception documentation.

The method of data capture is part of the record and can be accessed for reporting and audit purposes. In addition, the visit location type can be noted as residence, community center, etcetera. Location information is captured both at the beginning and end of each visit.

Captured data is compared to scheduled visit information as well as to authorized services to verify the visit meets pre-defined criteria. Once the captured data is verified or deviations are explained, the visit is eligible to be submitted for billing.

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.

Tellus EVV is built from the ground up to create HIPAA-compliant electronic 837 claim files that will be submitted to West Virginia MMIS for claims processing in compliance with all Medicaid filing requirements.

The production version of our industry leading SaaS-based EVV technology was designed and developed in collaboration with Florida's Agency for Health Care Administration (AHCA). Today Tellus EVV confirms service delivery for thousands of visits per day. Service delivery data is verified near real time based on parameters defined by AHCA and qualifying claims are submitted to FL MMIS in the form of a Medicaid-compliant 837P daily. Daily workflow is:

1. MMIS transmits daily batch files to Tellus: Providers, Members, Prior Authorizations
2. Provider Administrators schedule visits using our web based EVV Console
3. Direct care workers access schedules on their personal or company-owned mobile devices
4. Rendered service data is captured by the direct care worker using GPS-enabled technology at the point of service
5. Provider Administrators have near real-time access to the status of scheduled and rendered services through the EVV Console
6. Business intelligence rule-based technology compares rendered services to scheduled services and prior authorized services
7. Provider Administrators review claims and manage them based on claim status:
    a. Matched-On Hold = Review and Submit for claims adjudication
    b. Unmatched-On Hold = Review, Remediate, Re-Match, Repeat or Submit for claims adjudication
    c. Submitted claims are transmitted to MMIS daily for adjudication
8. Claims adjudication results are transmitted from MMIS to Tellus weekly in the form of an 835
9. Submitted claim status in EVV is changed to either Paid or Denied

This workflow can be modified based on the requirements of DHHR using a combination of adding new business rules to our business intelligence rules engine and modifying parameter and configuration settings.

PG012	4519	1	The solution should automatically generate all required correspondence to individuals.

The Tellus EVV solution includes a built-in secure messaging exchange between provider administrators and direct care workers. System messages such as user credentialing can be auto-generated to be delivered to individual users via email and or text.

PG013	4523	1	The Vendor should provide correspondence metric reports upon request by the Department.

Tellus agrees to provide correspondence metric reports on any available data as requested.

PG014	4552	1	The solution should assist users in identifying which sections of forms should be filled in manually.

Tellus agrees to provide messaging to assist users in identifying which sections of forms should be completed manually.

PG015	4582	1	The solution should provide the ability to deliver reports as mutually agreed-upon with the Department.

Tellus delivers robust reporting and analytics capabilities and agrees to deliver reports as mutually agreed-upon with the Department. In addition to pre-defined, standard reports, Tellus can customize reports based on customer requirements and formatting preferences.

Reports can be scheduled to run periodically and delivered. They can also be exported in a variety of formats to support data analysis and to supplement presentations. Access to reports and reporting tools is granted based on user role permissions.

PG016	4381	1	The solution should provide flexible web-based reporting, including ad hoc reporting of all data stored within the solution.

Tellus delivers robust reporting and analytics capabilities and provides features and functions to support ad hoc reporting of data stored within the solution. In addition to standard, stored reports users can customize reports and run them on a self-service basis.

Reports can be run on-demand near real time per user request. They can also be exported in a variety of formats to support data analysis and to supplement presentations. Access to reports and reporting tools is granted based on user role-based permissions.

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.

PG018	4888	2	Member receiving services
PG019	4889	2	Direct care worker
PG020	4890	2	Provider
PG021	4891	2	Location of visit
PG022	4892	2	Date of visit
PG023	4893	2	Start time of visit
PG024	4894	2	Missed visits
PG025	4895	2	Late visits
PG026	4896	2	End time of visit
PG027	4897	2	Visit late time
PG028	4898	2	Services provided
PG029	4900	2	Manual or electronic verification

All data captured by Tellus EVV is available for reporting on both a scheduled and ad hoc basis. Tellus EVV is operational and electronically captures all the data elements outlined in the detailed specifications referenced above. Some of these data elements are required by the 21st Century Cures Act, others are natively built into the core functionality of our EVV solution and several will be derived based on the specific requirements for DHHR's EVV program implementation.

Tellus is fully compliant with the 21st Century Cures Act mandate capturing the following required data points for home and community-based personal and home health care services provided through a Medicaid state or waiver plan:

- Member receiving service
- Direct care worker providing service
- Location of visit

- Date of service
- Visit start time
- Visit end time
- Services provided

In addition, Tellus EVV natively captures the following additional data points required by DHHR:

- Provider
- Missed visits
- Late visits
- Visit late time
- Manual or electronic verification

During the solution planning phase Tellus will collaborate with DHHR and MMIS to define the criteria related to the remaining data points referenced in the detailed specifications:

- Missed visits – DHHR will define the parameters for a missed visit. For example, the rule may state, if a visit is scheduled for February 15th and the direct care worker has not started the visit by midnight of February 16th, the visit is labeled "Missed".
- Late visits – DHHR will define the parameters for a late visit. For example, the rule may state, if a visit is not started by the direct care worker within one (1) hour of the scheduled visit time, the visit is labeled "Late".
- EVV data collected and aggregated will identify the method of visit verification and retain the original data source and whether it was captured by the DHHR selected EVV solution or a 3rd party vendor, including the identity of the vendor.

All data is captured electronically and available for periodically scheduled and ad hoc reporting.

PG030	4604	1	The solution should have the ability to use identifiers, mathematical functions, formatting, and manipulate data within reports.

During the solution planning phase of the engagement Tellus will collaborate with DHHR to define reporting criteria in detail. Tellus employs a full-featured modular reporting tool capable of using identifiers, mathematical functions, formatting and other forms of data manipulation within reports. Reports can also be exported to excel for data manipulation and analysis.

Tellus offers a library of reports that are part of our standard solution and offered on a scheduled and ad hoc basis. In addition, Tellus can build reports required by DHHR and train users with reporting permissions how to run ad hoc reports.

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.

Our business intelligence rules engine can ensure direct care services do not overlap with other direct care services. In our standard implementation, a direct care worker cannot be logged into more than one visit at a time. If more than one member is being treated by one direct care worker at the same time, the members must be scheduled on the same visit record by an administrator, this is typically indicated as an option by the utilization management contractor appending a billing modifier to the prior authorized service code(s).

This is currently the only mechanism that allows one direct care worker to provide overlapping services with data that is electronically captured using Tellus EVV and is easily disabled if DHHR does not wish to permit this option.

In some of the programs using Tellus EVV, there are times when it is necessary for two direct care workers to deliver services to one member at the same time. Each care provider is independently scheduled and logged into the visit. Administrators will be able to see the two visits in progress both real time in using reporting tools. Business intelligence rules confirm this is allowable based on criteria defined by program administrators, utilization management contractors and MMIS. Only visits meeting defined criteria are available to be submitted for claims adjudication processing.

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.

Tellus EVV utilizes a modular data aggregation engine to compile information from all EVV data sources and calculates total daily and weekly hours worked by direct care workers and agencies. This information is available for reporting on a periodic and ad hoc basis. If desired, business intelligence rules can be written to flag specific circumstances. For example, if DHHR wants to be alerted if a provider is scheduled to work more than 8 hours in one day, that data can shared when a provider agency creates a schedule triggering that rule.

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.

Tellus EVV modular components include a business intelligence rules engine and a data aggregation engine. These modules offer a high degree of flexibility and extendibility that can incorporate rules related to retroactive care plan changes for specific programs and/or services. Tellus will work with DHHR and MMIS to better understand this requirement during the solution planning phase of the engagement.

PG034	4210	1	The solution should allow the Department to define and limit the circumstances in which a manual verification can be made.

Tellus EVV provides the ability for DHHR to limit the circumstances in which manual verification is allowed using a combination of business rules and user permission-based roles that will be defined during the solution planning phase of the engagement.

Permission-based roles define which users can perform manual overrides. Administrators may be given permission to enter visit start and end times in the Administrator Console on behalf of the direct care provider. They also may be required to enter reason codes to

explain why data cannot be captured remotely and/or why rendered service data may not agree with scheduled information.

The method of data collection, (electronic or manual), and manual overrides of data captured electronically are monitored using an audit log that records the user who made the change and the date and time the change was made.

Business rules can be written flag manual data entry as a deviation from expected activity so DHHR can be made aware of deviations from expected behavior in the form of alerts or reports.

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.

Tellus EVV can use eligibility data transferred from MMIS to determine if waiver requirements apply to a specific service based on plan, program, service code, modifier and/or member criteria. If no waiver requirements apply, business intelligence rules can be written to assume state plan requirements apply to a specific service rendered to a member.

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.

Tellus has reviewed the high-level program requirements in DHHR RFP and is confident in

our ability to understand detailed requirements for each waiver and other state program requirements to develop and propose system edits that will meet the needs of DHHR.

Tellus will propose business rules, configuration settings and parameters to incorporate at the implementation of the solution and during the operational phase of the engagement. Tellus will review and propose system edits and settings for consideration at the interval defined by DHHR.

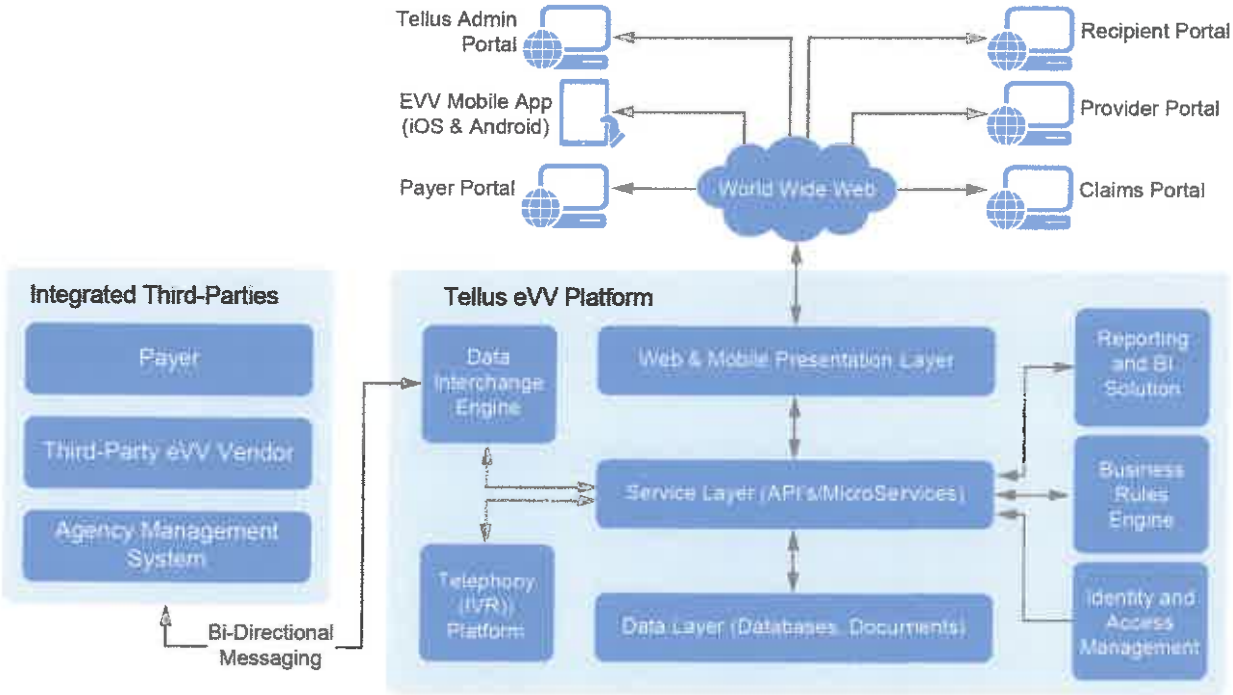
Tellus EVV is flexible and adaptable to different business processes based on the needs of individual DHHR programs.

PG037	4834	1	The Vendor should provide web portal functionality that addresses the needs of:
PG038	5013	2	Provider agencies and their direct care workers
PG039	5224	2	Members
PG040	5225	2	Waiver program and/or legal representatives
PG041	5014	2	State program staff

Tellus EVV provides web-based portal functionality available to provider agencies, direct care workers, members, legal representatives and state program staff. The web portal is available using commercially available hardware and standard web browsers. For example:

DESCRIPTION	CAPABILITY
Supported PC Operating Systems	Windows OS (32 or 64 bit) Version 7 or higher Mac OS Version X (10) or higher
Supported PC & Mac Browsers	Microsoft Internet Explorer Version 11 or higher Microsoft Edge Version 16 or higher Google Chrome Version 4 or higher Apple Safari Version 10 (Mac)/4 (Windows) or higher Mozilla Firefox Version 57 or higher

Constituents accessing data through the portal will be restricted to the information they can see and change based on role-based permissions. The following image provides a high-level overview of our solution architecture:



Users, including DHHR, other payers, provider agency administrators, direct care workers, members and legal representatives login to the solution via the world wide web and are able to access the data they are authorized to review, modify and/or report on near real

time. User profiles and permissions are designed to provide each user with only the information to protect PHI and other sensitive data.

1.3 PROGRAM INTEGRITY

PI001	4002	1	The solution should allow the Department the ability to view the same information as a service provider.

Tellus EVV Payer Portal provides DHHR with access to the complete set of business data through reports, dashboard cards, and ad-hoc reporting. DHHR will have the ability to view the same information as a service provider. Information is available to DHHR and the service provider near real-time.

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.

Tellus EVV can provide a summary of direct care workers and provider agencies who demonstrate a high level of missed visits, late visits, potentially fraudulent services and potentially fraudulent billing patters as requested by DHHR.

One of the ways this can be accomplished is by defining default settings include tolerance levels for late or missed visits (in terms of minutes elapsed from a missed caregiver clock-in). Analytics can be employed to establish averages and identify direct care workers and provider agencies with a greater than average percentage of late or missed visits. Alternatively, direct care workers and provider agencies can be ranked based on their percentage of late or missed visits and DHHR can review to determine unusual patterns.

Potentially fraudulent activity can be flagged by identifying direct care workers and provider agencies with high levels of manual data capture and/or overrides or the overuse of specific reason codes.

Tellus will work with DHHR and MMIS to understand areas of concern and vulnerability and make recommendations related to business rules, user-based roles and permissions, system configurations and system edits to capture, flag and report activities indicative of undesirable behaviors.

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.

Tellus EVV tracks time, location and tasks associated with services provided by direct care workers at the point of service to safeguard against fraud as well as to improve service delivery and program oversight. Our solution is designed to be minimally burdensome to direct care workers and members; however, is fully compliant with the 21st Century Cures Act mandate capturing all required data points as well as other important to member quality of service and direct care worker accountability. All captured data is available to DHHR near real time for care management oversight and to monitor program integrity as well as guard against the opportunity for fraud, waste and abuse.

PI004	3991	1	The solution rules/procedures should have the ability to ensure the same direct care worker is not providing services to multiple members at the same time at different locations.

Our EVV solution ensures the same direct care worker cannot provide services to multiple members at the same time at different locations because a direct care worker cannot be logged into more than one visit at a time.

If more than one member is being treated by one direct care worker at the same time, the members must be scheduled on the same visit record by an administrator. Each visit record can be scheduled at only one start address and one end address. In our current implementation, scheduling more than one member at the same time and location is indicated as an option by the utilization management contractor appending a billing modifier to the prior authorized service code(s).

When the visit is completed the data is matched against prior authorized services and scheduled services to ensure the criteria matches. If it does, the visit can be submitted for claims adjudication purposes. If not, the visit information must be changed and/or a reason code must be added by the provider agency administrator prior to submitting the visit for claims adjudication purposes. All information entered or modified in Tellus EVV is captured in an audit log that retains the change, the user and the date the data is entered or modified.

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:
PI006	5208	2	Payers
PI007	5209	2	Programs
PI008	5210	2	Provider Agency
PI009	5211	2	Direct care workers
PI010	5212	2	Members

Tellus EVV delivers, role-based reporting capabilities providing users with the ability to review, analyze and report all data across categories on a monthly basis. Data can be reported by:

- Payer
- Program
- Provider agency
- Direct care worker
- Member

In addition to standard reports, Tellus can customize reports based on DHHR requirements and formatting preferences. Reports can be scheduled to run periodically as well as on an on-demand, ad-hoc basis. Reports can also be exported in a variety of formats to support

data analysis and to supplement presentations. Access to reports and reporting tools is granted based on user role permissions.

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.

Tellus EVV electronically captures all data input by the direct care worker. This includes data elements are required by the 21st Century Cures Act as well as others that are required by DHHR. At the time the information is entered, the following metadata is also captured:

- Method of entry
  - Electronic
    - GPS-enabled
    - IVR
    - Other, (if allowable)
  - Manual
    - Provider agency administrator
    - Direct care worker override, (if allowable)
- Source of Data
  - DHHR selected EVV vendor
  - Identity of 3rd party vendor

If any of the information entered in the EVV solution by the direct care worker is changed or modified, Tellus EVV records in an audit log:

- Change made to the record
- User who made the change
- Date the data is changed
- Reason the change was made

All data elements and audit log activity are available for reporting and analysis to eligible users.

ATTACHMENT 8: TECHNICAL SPECIFICATIONS APPROACH

Instructions: 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. 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 specifications included in RFP ***Section 4: Project Specifications.*** 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. 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.

2 DATA SOURCES, DELIVERY AND DISPLAY

DD001	5115	1	The Vendor should develop and provide to the Department a Logical Data Model (LDM) that includes, but is not limited to:
DD002	5116	2	Data classes
DD003	5117	2	Attributes
DD004	5118	2	Relationships
DD005	5119	2	Standards
DD006	5121	2	Other data elements identified by the Department

Tellus will develop and submit all required technical documentation, including a final

architectural diagram for each system environment. One of the components of the solution architecture documentation will be the Logical Data Model, (LDM) with a full data dictionary defining: data classes, attributes, relationships, standards and other data elements required by DHHR.

In addition to the specific requirements outlined above, our standard documentation includes: a data mapping crosswalk, inbound/outbound capability, frequency for all interfaces and a high-level process flow diagram.

During the Solution Planning and Solution Design, Testing and Operational Readiness phases of the engagement, the technical documents will evolve as the business requirements are defined, refined and tested. Tellus is committed to working with DHHR to ensure all requested solution documentation meets the criteria, delivery timelines and quality standards expected.

DD007	4088	1	The Vendor should provide a complete list of data elements along with corresponding definitions for reporting purposes, upon request.

Upon request, Tellus will provide a complete list of data elements along with corresponding definitions for reporting purposes. At a minimum, the data dictionary will contain:

- Data classes
- Data attributes
- Data relationships
- Field name
- Field description
- Database field name
- Database table
- Field type and length
- Codes associated with the field
- Descriptions of each code

Tellus will work with DHHR to ensure data definitions are clear and support reporting initiatives.

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.

Tellus EVV is comprised of five major modules, or components. The modules work seamlessly together with data captured in one component available near real time throughout the solution. This remote access to information as it is being collected provides real time insight to services as they are being provided which facilitates the ability to oversee user activity.

As an example, a direct care worker, Jesse - arrives at the home of Sandy, a new member, and starts the visit scheduled for 10 am at 10:05 on their mobile device using the Tellus EVV mobile app. At 10:05, the visit status on the provider administrator dashboard changes from "scheduled" to "in progress". Tom, the provider administrator who is 20 miles away sitting at his desk knows Sandy is in good hands.

Alternatively, if the DHHR business rules state a visit is late if it is not started at the precise time the visit is scheduled to begin, John, the provider administrator will see Sandy's visit status change from "scheduled" to "late" at 10:01. As soon as Tom sees Jesse did not begin the visit on time, Tom calls Jesse to find out why the visit has not been started and finds out Jesse is parking in Sandy's driveway and will be starting the visit momentarily. At 10:05 Tom sees the visit status change from "late" to "late, in progress".

The same information is also available real time to care managers and other eligible users through the payer portal. It is also retained for ongoing analytical and reporting purposes.

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 integration and aggregation are core components of Tellus EVV. Our open source data sharing tool allows data to be easily shared employing a variety of industry recognized standards and protocols including real-time data sharing for both individual and batch transactions.

Data from third-party EVV vendors is imported into Tellus EVV to provide a comprehensive data analytics and reporting solution for your EVV program. Tellus works with third party vendors by providing standard data sharing specifications and protocols that are tested and implemented to ensure data collected across the EVV ecosystem is normalized to support program goals. Tellus meets third party vendors where they are by accepting data in formats ranging from periodic batch transmissions delivered via SFTP servers to application protocol interfaces (APIs) delivered via web services. Data sharing options for the WV EVV solution will be tailored to meet the specifications outlined by DHHR.

Once visit data is received it is compared to scheduled and authorized services to ensure it is compliant with EVV requirements. Visit data meeting the criteria defined by DHHR will be submitted to MMIS in the format and at the frequency requested.

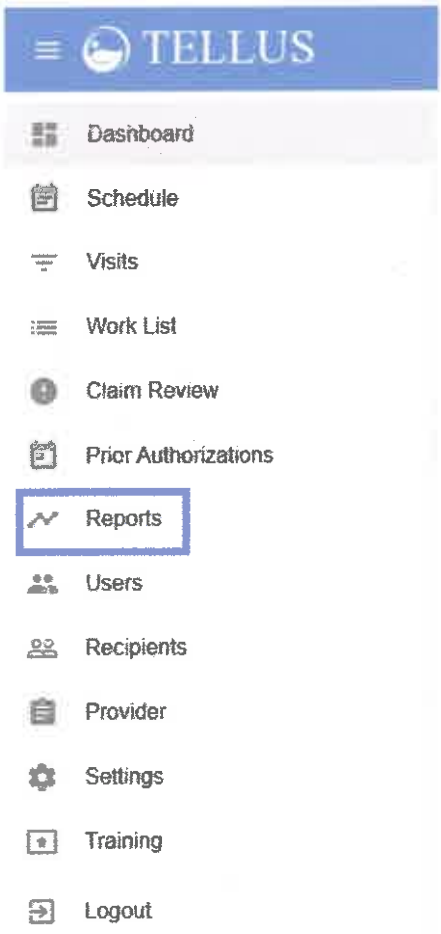
DD010	4513	1	The solution should have the ability to integrate client data for all programs served by the solution into the Master Data Management (MDM) platform.

Tellus EVV integrates client data for all supported programs into our Master Data Management (MDM) platform. Our solution natively creates a master client index, also known as a globally unique identifier (GUID) for each member. The unique identifier is created by concatenating key business data for each member to create an internal database GUID key. As an example, the combination of Medicaid ID and Date of Birth for a specific member may be used to create the internal database GUID key. This ensures all

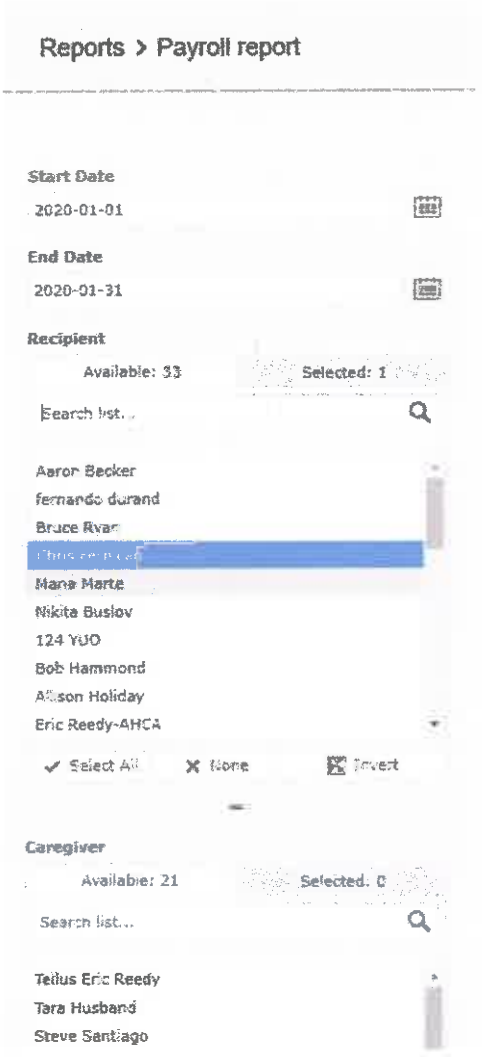
member data received during the contract period will be related even if the member is receiving services under multiple programs.

DD011	4585	1	The solution should allow users to extract data, manipulate the extracted data, and specify the desired format of the output.

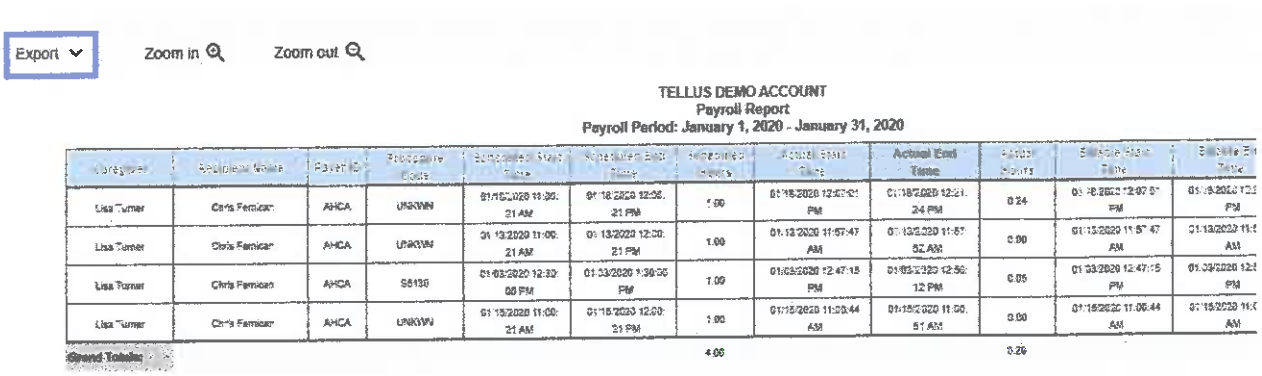
Tellus EVV boasts robust reporting and analytics capabilities. Standard reports and ad hoc reporting functionality are available to all eligible users through web-based consoles.



They are easily customizable to tailor user needs by using intuitive filters:



Once filters are selected, the report is run and can be viewed online or exported in a variety of formats for review, analysis and presentation purposes:

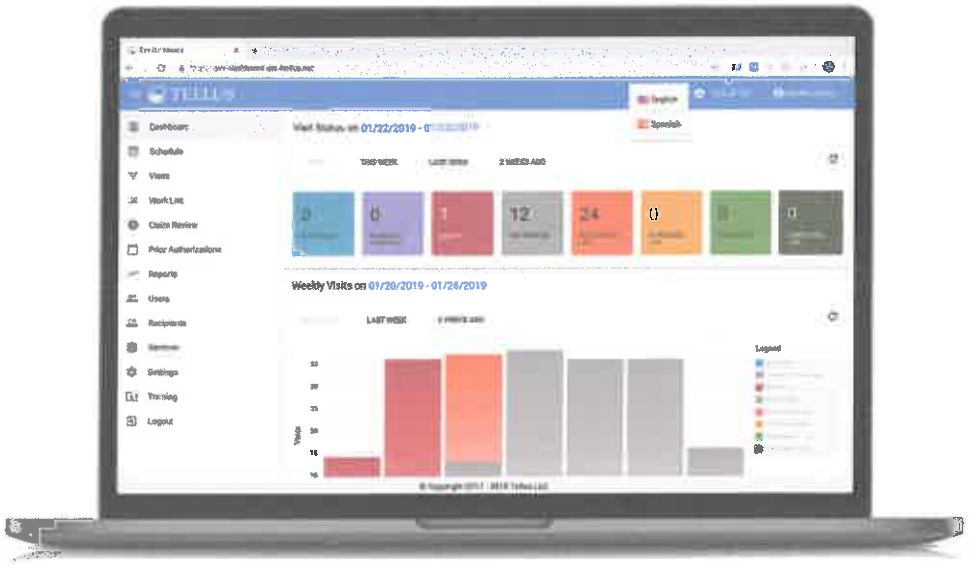

Export Zoom in Zoom out

TELLUS DEMO ACCOUNT
Payroll Report
Payroll Period: January 1, 2020 - January 31, 2020

Caregiver	Recipient Name	Payer ID	Procedure Code	Scheduled Start Time	Scheduled End Time	Scheduled Hours	Actual Start Time	Actual End Time	Actual Hours	Billable Start Time	Billable End Time
Lisa Turner	Chris Fernican	AHCA	UNKWN	01/15/2020 11:30:21 AM	01/15/2020 12:06:21 PM	1.00	01/15/2020 12:03:01 PM	01/15/2020 12:21:24 PM	0.24	01/15/2020 12:07:01 PM	01/15/2020 12:21:24 PM
Lisa Turner	Chris Fernican	AHCA	UNKWN	01/13/2020 11:00:21 AM	01/13/2020 12:00:21 PM	1.00	01/13/2020 11:57:47 AM	01/13/2020 11:57:52 AM	0.00	01/13/2020 11:57:47 AM	01/13/2020 11:57:52 AM
Lisa Turner	Chris Fernican	AHCA	S5130	01/03/2020 12:30:00 PM	01/03/2020 1:30:00 PM	1.00	01/03/2020 12:47:15 PM	01/03/2020 12:50:12 PM	0.05	01/03/2020 12:47:15 PM	01/03/2020 12:50:12 PM
Lisa Turner	Chris Fernican	AHCA	UNKWN	01/15/2020 11:00:21 AM	01/15/2020 12:00:21 PM	1.00	01/15/2020 11:00:44 AM	01/15/2020 11:00:51 AM	0.00	01/15/2020 11:00:44 AM	01/15/2020 11:00:51 AM
Grand Totals:						4.00			0.29		

Reports can be exported into excel, csv or pdf file formats. Once exported data can be analyzed, modified and/or included in presentations.

In addition Tellus supports a payer dashboard for consolidated reporting across participating provider agencies. The payer dashboard displays tiles that can be drilled into to apply filters and obtain more granular information that can be exported for review, analysis and reporting. More sophisticated users can be trained develop and run ad hoc reports on demand.



If DHHR desires the ability to extract data in other methods, those requirements will be elicited during the solution planning phase of the engagement.

DD012	4769	1	The solution should provide required Federal and Department data sharing including high-speed data transfer functionality to send and receive information.

Tellus supports the open/hybrid EVV model and is fully compliant with Center for Medicaid Service (CMS) standards including data sharing supported by high-speed data transfer functionality to send and receive information.

Tellus publishes standard open Application Program Interfaces (APIs) promoting interoperability across the Medicaid ecosystem by integrating with care management applications, third-party EVV vendors and MMIS.

Bi-directional interfaces are supported, built and managed using our integration engine and can support data sharing intervals required by DHHR up to real time. All data sharing

across the Tellus EVV solution is real time unless the mobile application is being used in a location that does not have access to WiFi. If that is the case all visit data is captured and securely stored on the direct care workers mobile device until access to WiFi is regained. At that point, the visit data automatically syncs with the Tellus EVV database and the visit data is available across the platform.

Our standard data sharing tool allows data to be shared employing many standards and protocols including near real-time data sharing for both individual and batch transactions. Our business intelligence rules engine applies rules to visits and claims data for tracking service utilization and comparing it to prior authorization data. This data is available to those who have permission to view it in the web-based consoles.

DD013	3997	1	The solutions rules/procedures should allow for electronic communication between the Department, fiscal/employer agents, and providers.

Tellus EVV supports data sharing in a variety of ways. Communication protocols are primarily focused on direct care workers providing status updates to providers; however, our product roadmap includes a "provider message board" function that will allow for the Department to communicate with providers and fiscal employer agents. This functionality will be in production in time for the DHHR implementation.

DD014	5138	1	The solution should have the ability to store member communications.

Tellus EVV stores all data and communications based on the terms of our agreements. Information is available online for a minimum defined period and then archived for the term of the contract plus the required data retention period. All communications that are transmitted between providers, fiscal employer agents, DHHR, caregivers, and members are archived.

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 exchange and aggregation is a core competency for Tellus. As a strong proponent of the open/hybrid EVV model, Tellus publishes standard open Application Program Interfaces (APIs) promoting interoperability across the Medicaid ecosystem by integrating with care management applications, third-party EVV vendors and MMIS. Tellus is committed to developing interfaces with all parties deemed relevant by DHHR.

Our dedicated integration teams are specifically assigned to working with trading partners to define, write, support and manage data exchange channels using our industry-leading, cross-platform, bi-directional, health care integration engine.

The purpose of data sharing is to consolidate data from various sources into a system of record in the most efficient manner possible to save time and minimize redundant processes. Sharing data with other systems means data is transmitted or exported from one software application and shared by import into another application. As it relates to EVV, we import data from multiple systems to store data in a common database. Some of this information is foundational to set up the system; for example, the MMIS will send provider, member and prior authorization data to import into the EVV database. Visit data collected from our solution as well as other EVV systems is imported into the data aggregation database and transmitted in real-time transactional or batch mode.

When foundational information is loaded, providers will have the information they need to schedule visits for members. Business intelligence rules formulated by program and payer administrators are run against transaction data to determine the validity of delivered services. Transactions in the form of visits, regardless of the original source, that violate the rules associated with a specific program or payer can be remediated by the provider and the transactions will be reevaluated. Those visits with violations are flagged and show up in exception reports. Compliant visits are transferred in EDI files to MMIS for claims adjudication. Adjudicated claims data can be received by Tellus so providers can review the status of their submitted claims in their EVV portal.

DD016	4398	1	The solution should have the ability to interface with West Virginia's Enterprise Service Bus (ESB).

Tellus EVV is supported by a service-oriented architecture which making it easy to adapt to the unique configuration requirements of DHHR. The Tellus integration team will work with DHHR and your vendors to understand the specifications to successfully integrate with West Virginia's Enterprise Service Bus (ESB). Tellus can accomplish this goal using a variety of standards and protocols and will implement the interface to accommodate the standards, protocols and frequencies favored by DHHR.

DD017	3966	1	The Vendor should complete, subject to approval by the Department, the interface with the Medicaid Management Information System (MMIS).

The Tellus EVV platform is built on a service-oriented architecture (SOA) and is open database connectivity (ODBC) compliant making the application extremely flexible and agile while allowing for bi-directional exchange of information with virtually any other open architecture application, including Medicaid Management Information Systems (MMIS).

Tellus is in production sharing data with MMIS in other states. Data transfers and aggregation are core competencies of Tellus. In fact, we have dedicated integration teams specifically assigned to data sharing and integration. We use industry-leading, cross-platform, bi-directional, health care integration engines for data interchange.

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.

Our open source data sharing tool allows information to be easily transmitted and received employing a variety of industry recognized standards and protocols in asynchronous as well as synchronous real-time modes for both individual and batch transactions.

Data sharing transmission options for the WV EVV solution will be tailored to meet the format and frequency specifications outlined by DHHR.

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.

Tellus EVV can receive provider, member and prior authorization data from MMIS at the frequency and format determined by DHHR.

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).

Tellus EVV is able to apply pre-edit information and serve as a data source for purposes of applying edits during claims processing. Typical daily workflow is:

1. MMIS transmits daily batch files to Tellus: Providers, Recipients, Prior Authorizations
2. Provider Administrators schedule visits using our web based EVV Console
3. Care providers access schedules on their personal or company-owned mobile devices
4. Services rendered are confirmed using GPS on the direct care providers' mobile devices
5. Provider Administrators have real-time access to the current status of scheduled visits on our EVV Console
6. Matching algorithms run in the background every ten minutes comparing: scheduled services, rendered services, prior authorizations
7. Provider Administrators review claims and take action. Claims statuses and related actions are:
    a. "Matched-On Hold" – Review and "Submit"
    b. "Unmatched-On Hold" – Review, Remediate, Matching Algorithm Runs again and either promotes to "Matched-On Hold" or retains "Unmatched-On Hold" status

c. "Submitted" claims are transmitted to FL MMIS or MCO daily for adjudication

8. Claim Resolution file is transmitted to Tellus weekly, Tellus stamps "Submitted" claims as "Paid" or "Denied"

Provider and Payer reports are available on the EVV Console at every step of the process for the duration of the term of the engagement.

DD022	3952	1	The solution should accept individual and/or batch visit verification inquiries from the Medicaid Management Information System (MMIS).
DD023	4912	2	Member name
DD024	4913	2	Billing provider
DD025	4914	2	Name
DD026	4915	2	Date
DD027	4916	2	Time of service delivery

Tellus EVV can accept individual and/or batch visit verification inquiries from MMIS. The format of the inquiries will be defined by DHHR during the solution planning phase of the engagement. Our data integration team will work with DHHR and MMIS to support the format and frequency requested to share visit verification information including:

- Member name
- Billing provider
- Name
- Date
- Time of service delivery

This information is also available and accessible on demand to eligible users through the DHHR payer dashboard.

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.

Tellus EVV can provide visit information to MMIS by individual and/or in batch format at the discretion of DHHR. This information is available in both machine and human readable formats. Real-time rendered service data is typically evaluated in the EVV solution for claims pre-adjudication. Once visit verification data is validated, claims data is submitted to MMIS in the form of an EDI-compliant 837.

Visit information is also available in human readable form using the payer and provider dashboards. Eligible users and access and review this information online and/or in the form of reports that can be exported review and analysis.

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/)

Tellus EVV supports obtaining member eligibility information through MMIS using industry standard interfaces and exchange via EDI X12N 270/271.

DD030	5153	1	The solution should conform to ASC X12 Technical Reports Type 3 (TR3), Version 005010. (Reference: http://www.wpc-edi.com/)

Tellus EVV complies with ASC X12 Technical Reports Type 3 Version 005010 implementation guides, as amended by payer-specific companion guides.

DD031	4475	1	The solution should generate all forms and notices as necessary.

Tellus EVV will be configured and enhanced, as necessary, to generate and share communications and notices in all forms required by DHHR.

DD032	4206	1	The solution should have the ability to schedule alerts and user notifications.

Tellus EVV natively supports the ability to schedule and deliver alerts and notifications to users, examples include:

- Account alerts - user credentialing, password reset
- Business alerts - new PA, Visit being scheduled with no PA
- Care alerts – Member concern reported by direct care worker to provider

The content and form of notifications and alerts will be defined during the solution planning phase of the engagement for the implementation of the system and can be modified during the term of the contract.

DD033	4470	1	The solution should allow printing of blank and completed documents including, but not limited to:
DD034	4935	2	All forms
DD035	4936	2	All system-generated correspondence
DD036	5104	2	Reports

Tellus EVV supports the printing of blank and completed documents including forms, correspondence and reports. Reports can typically be either printed or downloaded in a variety of formats including csv, excel and pdf.

DD037	4481	1	The solution should generate and supply forms in the following methods, including, but not limited to:
DD038	4482	2	Email
DD039	4483	2	Download from Portal
DD040	4484	2	Postal Mail, upon request by the Department

Tellus EVV supports the printing and downloading of forms. Downloaded reports can be delivered via email or postal mail.

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.

Tellus will work with DHHR to define forms and their field attributes during the solution planning phase of the engagement for implementation purposes. Forms and field attributes can be modified during the term of the contract as requested by DHHR.

DD042	4478	1	The solution should allow updates to form templates as directed by the Change Management Plan.

Tellus will work with DHHR to define form templates during the solution planning phase of the engagement for implementation purposes. Forms templates can be modified during the term of the contract as requested by DHHR.

DD043	4479	1	The solution should group related correspondence to ensure materials are delivered in a single mailing or posted to a portal account.

Tellus will work with DHHR to define and implement correspondence grouping rules so that related items will be delivered and/or presented in a logical manner.

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.

Tellus will work with DHHR to define and deliver data files containing forms and notices to their printing vendor for monthly distribution.

DD045	4487	1	The solution should automatically populate information on notices or forms being issued.

Tellus EVV can be configured to automatically populate information on notices or forms being issued as requested by DHHR.

DD046	4490	1	The solution should generate batch forms.

Tellus EVV can be configured to generate batch forms as requested by DHHR.

DD047	4493	1	The solution should save delivered forms to the user's account.

Tellus EVV can save user specific correspondence to the user's account. Tellus will work with DHHR to define and implement criteria to save and share data in accordance with privacy laws.

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.

Tellus EVV can deliver data files containing all correspondence defined by DHHR to their designated vendor at the frequency and in the format requested.

DD049	4527	1	The solution should post finalized correspondence to the web portal, according to the Department's business rules.

Tellus EVV will post finalized correspondence to the web portal according to DHHR business rules.

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.

Tellus EVV has the ability to produce correspondence in printer-friendly 8.5" x 11" formats in both landscape and portrait orientation.

DD051	4537	1	The solution should have the ability to automatically save a Portable Document Format (PDF) copy of each final correspondence.

Tellus EVV can store and export documents in several formats including: csv, excel, pdf, and tiff.

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.

Tellus EVV allows users to select their preferred method of correspondence including email, post mail, text and phone. Note: Some types of correspondence may not be suitable

for email over the public internet due to privacy and security requirements related to PHI.

DD053	4544	1	The solution should generate correspondences using pre-defined templates.

Tellus EVV generates correspondence using pre-defined templates.

DD054	4546	1	The solution should include automatic system-generated correspondence with output capabilities including, but not limited to:
DD055	4960	2	Email
DD056	4962	2	Post to user portal account
DD057	4963	2	Queue for printing

Tellus EVV supports automatic system-generated correspondence with output capabilities including email, portal access and print queues. Note: Some types of correspondence may not be suitable for email over the public internet due to privacy and security requirements related to PHI.

DD058	4547	1	The solution should be able to schedule distribution of correspondence.

Tellus EVV can schedule the distribution of correspondence.

DD059	4561	1	The solution should provide flexible web-based reporting that meets external reporting needs and requirements defined by the Department.

Tellus EVV utilizes a modern, open source reporting tool that will be configured to meet all external reporting needs and requirements defined by DHHR.

In our standard implementation, Tellus EVV web dashboards are viewable on the EVV

Console. "Cards" are created that can be mixed and matched dynamically to customize the look and feel for the individual user of the dashboard based on user login credentials similar to the way users customize applications to launch when they start their computer. The power is in the hands of users with the following reporting capabilities:

Scheduled — Reports can be scheduled to run on a periodic basis and cached on the reports page for access by authorized users at any time.

Ad-Hoc — Ad-hoc reports can be created by users by accessing built-in, drill-down features accessible through the dashboard as well as by modifying filters on pre-defined reports.

Exports — All scheduled and ad-hoc reports can be exported in various formats including pdf, csv and excel.

The flexibility of creating and running reports in various ways with the ability to print or export data in a variety of formats is the perfect foundation to support DHHR reporting needs and requirements.

DD060	4085	1	The solution should include a standard library of reports that can be generated by any user with appropriate access.

Tellus delivers robust reporting and analytics capabilities including a standard library of reports that can be generated by any user with appropriate access. Our standard reporting library includes:

	Fraud Detection	Aberrant Billing	Service Delivery	Logistics
Activities across providers	✓	✓	✓	✓
Claims by date				✓
Claims edited	✓	✓	✓	
Claims exceptions by reason code	✓	✓	✓	✓
Claims on hold	✓	✓		✓
Claims resubmitted	✓	✓	✓	
Claims submitted, denied	✓	✓	✓	
Claims submitted, paid				✓
Claims voided	✓	✓	✓	
Direct care giver schedule				✓
Prior Authorization, no scheduled visits			✓	
Provider ID does not equal authorized provider ID	✓	✓	✓	
Recipient address change	✓	✓	✓	✓
Recipient list				✓
Visits delivered, deviate from prior authorization		✓	✓	
Visits delivered, start address does not equal end address	✓	✓		✓
Visits late			✓	✓
Visits overlapping services	✓	✓	✓	✓
Visits scheduled	✓	✓	✓	✓
Visits scheduled address does not equal delivery address	✓	✓		✓
Visits scheduled, conflicting prior authorizations	✓	✓	✓	✓
Visits scheduled, no prior authorization		✓	✓	
Visits scheduled, not completed (missed)	✓	✓	✓	✓
Visits supported by third party EVV	✓	✓	✓	✓
Visits unable to complete	✓	✓	✓	

In addition to standard reports, Tellus can customize reports based on customer requirements and formatting preferences. Reports can be scheduled to run periodically as well as on-demand. They can also be exported in a variety of formats to support data analysis and to supplement presentations. Access to reports and reporting tools is granted based on user role permissions.

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.

Tellus EVV can display the number of pages in a report before the user proceeds with printing the report.

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:
DD063	4973	2	Excel
DD064	4974	2	Word
DD065	4975	2	Hyper Text Markup Language (HTML)
DD066	4982	2	Comma-Separated Value (CSV)
DD067	4984	2	Portable Document Format (PDF)

Tellus EVV supports the ability to export reports directly from our solution platform into user-specified formats. Export formats that are currently available are Excel, CSV and PDF. Additional formats can be accommodated upon DHHR request.

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.

Tellus EVV Business Intelligence tool includes online data visualization with click-to-drill-down to the underlying tabular data.

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.

Each Tellus EVV Payer has a dedicated payer database that includes:

- Recipient Data from Payer
- PA Data from Payer
- Provider Data from Payer
- Visit and Claims Data Generated by Tellus

The Tellus EVV Payer Portal is a Business Intelligence (BI) platform that provides Payers Access to this Data on a production read-replica database (near real-time).

Common Data Formats:

- Dashboard "Cards" - Graphic with drill down to tabular data.
- Traditional Tabular Reports – Exportable in many formats
- Ad Hoc Reporting – Exportable in many formats

DD070	4815	1	The solution should contain the following features and capabilities including, but not limited to:
DD071	4816	2	Drill down and look up functionality to minimize re-entry of information across multiple screens
DD072	4817	2	Multi-tasking and multiple window capability, including split screens

Yes, the data entry screens are organized to consolidate views and efforts. The user-facing PC solution is browser based.

DD073	4644	1	The solution should provide context-sensitive help to users on all screens.

Yes, all screens contain context-sensitive, multi-lingual tool tips.

DD074	4818	1	The solution should provide menus that are understandable by non-technical users and provide secure access to all functional areas.

The Tellus EVV Mobile App, EVV Administrator Console and EVV Claims Console solutions are fully integrated, intuitive and user friendly. Consoles have expandable/collapsible left-hand menus as well as a breadcrumb trail, so users can step back through pages rather than going back to the menu The menu is easily accessible but only needed for changing the password, system settings, accounts, user profile updates, and logging out.

DD075	4859	1	The solution should provide a user interface that allows users to move easily throughout the system.

The Tellus EVV Mobile App has icons at the bottom of the page that allow users to view their schedule (Home) in several formats (day/week/month), recipients and messages. The menu is easily accessible but only needed for changing the password, system settings, accounts, user profile updates, and logging out.

We have designed appealing user interfaces with:

- Readable fonts
- Consistent colors
- Large buttons
- Limited number of steps to accomplish the goal

DD076	4839	1	The solution should have the ability to provide public information without requiring authentication for the web portal.

Yes, the solution does include the capability to make select pages that contain only public information available to anonymous users.

DD077	4862	1	The solution should provide user interface features and capabilities including, but not limited to:
DD078	4863	2	Pull-down menus and window tabs
DD079	4864	2	Scalable, true-type screen and printing fonts
DD080	4865	2	Uppercase and lowercase alphabetic characters
DD081	4866	2	Ability to tab and mouse-click through data fields and screens
DD082	4868	2	Consistent theme throughout the site and standardize all headings and footers with index tabs as identified by the Department
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

The Tellus EVV Mobile App, EVV Administrator Console and EVV Claims Console solutions are fully integrated, intuitive and user friendly. Consoles have expandable/collapsible left-hand menus as well as a breadcrumb trail, so users can step back through pages rather than going back to the menu. The mobile app has icons at the bottom of the page that allow users to view their schedule (Home) in several formats (day/week/month), recipients and messages. The menu is easily accessible but only needed for changing the password, system settings, accounts, user profile updates, and logging out.

We have designed appealing user interfaces with:

- Readable fonts and use of upper/lowercase to improve readability
- Text can be scaled up or down using browser tools
- Consistent colors, graphics, and themes
- Large buttons
- Limited number of steps to accomplish the goal
- On our consoles, users can either click individual fields or tab through them

- Error messages are clear and concise and tell users exactly how to make corrections; error messages are available in English or Spanish depending on the language the user selects

DD084	4884	1	The solution should provide the capability to display confirmation messages for response and request transactions when interfacing with other systems.

When performing data interchange, Tellus always:

1. Returns an accepted/rejected response for every inbound transaction
2. Transmits an accepted/rejected count email to the sender
3. Processes accepted/rejected response from transmitter for every outbound transaction
4. Displays accepted/rejected status to end users via the user interface when applicable
5. Generates reconciliation reports for review with data interchange partner

DD085	4883	1	The solution should have the ability to allow users to download or print a copy of completed submitted forms.

Yes, the system allows for the display and print of any form that is uploaded to the system.

DD086	4347	1	The solution should have the ability to perform the following functions including, but not limited to.
DD087	4918	2	Create flags
DD088	4919	2	Send alerts
DD089	4920	2	Integration of alerts into the workflow
DD090	4921	2	Seamlessly integrate the generation of alerts in the workflow management process to a system user-defined group or individual

The Tellus EVV solution includes a messaging infrastructure that allows for communications, including user messages and alerts to be:

1. Triggered by any of a number of processes, including missed events, user interface activity, business events such as PA status.
2. Transmitted to one or multiple mobile and or web portal users or user roles via email, browser page inbox, or SMS.
3. Track whether messages and alerts have been viewed.
4. Long-term archived per data retention policies.

3 DATA QUALITY

DQ001	3993	1	The solution should provide a method to identify the following:
DQ002	5049	2	National Provider Identifier (NPI)
DQ003	5050	2	Healthcare Common Procedure Coding System (HCPCS)
DQ004	5051	2	International Statistical Classification of Diseases and Related Health Problems, 10th revision (ICD-10) and related modifiers
DQ005	5136	2	State-specific codes defined by the Department

Our solution requires that an NPI be entered for each payer; that identifier will be associated with

HCPCS Code/Mod(s) (service task codes and modifiers) uploaded to the system per DHHR specifications and can be selected when visits are scheduled. These codes are matched to prior authorizations and remain with the visit through claims processing and adjudication. Other state-specific codes can be accommodated as well.

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:
DQ007	5039	2	Definition of data elements

DQ008	5040	2	Data file formatting
DQ009	5041	2	Data exchange frequency
DQ010	5042	2	Thresholds for data quality and acceptance

Business rules, user roles and integrations developed during the business requirements gathering phase of the engagement are customized to the deployment.

Tellus EVV modules can be implemented coupled or uncoupled meaning they can each operate independently and integrated with applications built by other vendors. Data sharing can be real-time or provided based on a schedule in batch mode. For example, any data captured in Tellus EVV can be shared with:

- MMIS
- Enterprise service bus
- Data warehouses
- Other legacy systems

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.

During the business requirements gathering phase at the start of the program, the following information will be required at either the State or program level:

- Program Rules
- User Roles
- Role-based permissions
- System interfaces
- Interface criteria
- Mapping

- Rules
- Schedule
- Format
- Transmission protocols

Information gathered during this phase of the engagement will be used to create the Functional Requirements Document (FRD), which will be presented to the State for review and approval.

The Functional Requirements Document will serve as the foundation for the Detailed System Design Document (DSDD), which will describe how our EVV solution addresses the State's requirements.

Upon completion of the design and development of the application, we will deliver a User Acceptance Testing (UAT) / Testing, Validation and Operational Readiness (TV&OR) Plan to describe how the application was tested and to demonstrate it meets the functional requirements and is ready for implementation.

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.

Tellus has developed, published and maintains system interface standards for EVV data partners. Tellus will review our existing standards with DHHR and, if required, make changes to comply with DHHR standards.

DQ013	4771	1	The Vendor should ensure that file standardization is supported for data element lengths, field format, and type.

We will submit the technical documentation, including a final architectural diagram for each system environment, data dictionary, data mapping crosswalk, inbound/outbound capability, frequency for all interfaces and high-level process flow diagram prior to contract signature.

We will also negotiate the exact time frame for this delivery with the DHHR prior to contract signature. The DHHR will review and approve any architectural changes, relative to interface points with the DHHR and external data sources before we implement them.

We will implement integration point architecture changes in the lower environments first, and then promote them to upper environments after completing formal system integration testing (SIT) and user acceptance testing (UAT) and receiving the DHHR's approval.

The data dictionary will contain, at a minimum, each of the following fields in human-readable format:

- Field name;
- Field description;
- Database field name;
- Database table;
- Field type and length;
- Codes associated with the field;
- Descriptions of each code.

DQ014	4781	1	The solution should incorporate a method to view interface files for investigation and further processing.

Interface files are archived after processing, the most common method is to archive FTP files into a file directory or XML steam into object storage.

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

A complete snapshot of before and after transaction is captured for all interface activity on key business objects such as recipients, providers, caregivers, visits, claims, etc.

DQ016	4498	1	The solution should make information about data exchange errors and discrepancies available to the Department and appropriate users monthly.

When performing data interchange, Tellus always:

1. Returns an accepted/rejected response for every inbound transaction.
2. Transmits an accepted/rejected count email to the sender.
3. Processes accepted/rejected response from transmitter for every outbound transaction.
4. Displays accepted/rejected status to end users via the user interface when applicable.
5. Generates reconciliation reports for review with data interchange partner.

DQ017	4511	1	The Vendor should provide searchable data schemas and data dictionaries for the solution.

A data dictionary will be provided to DHHR and will contain, at a minimum, each of the following fields in human readable format:

- Field name;
- Field description;
- Database field name;
- Database table;
- Field type and length;
- Codes associated with the field;
- Descriptions of each code.

See sample data dictionaries here:
https://tellusolutions.atlassian.net/wiki/spaces/EVV/pages/85033179/Tellus+Message+Specifications

DQ018	4569	1	The solution should report on both duplicated and unduplicated record counts.

Duplicate records are identified during inbound transaction processing and returned to the transmitter in an accepted/rejected file report with error codes.

DQ019	4588	1	The solution should use consistent data schemes and version control.

Tellus operates on a consistent data schema that is managed through our source control management (SCM) process; all Tellus interfaces are fully documented.

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 to avoid duplicate data entry.

The Tellus EVV data model operates in a relational database that minimizes duplication of data through the use of foreign key data; in the event that there is a need for data to be synchronized then Tellus implements internal automated processes to do so.

DQ021	4571	1	The Vendor should maintain a comprehensive list of all reports, their intended use, and business area supported.

See following table is a list of key reports and the purpose of those reports. Tellus will work with DHHR to build additional reports defined during the solution planning phase of the agreement.

	Fraud Detection	Aberrant Billing	Service Delivery	Logistics
Activities across providers	✓	✓	✓	✓
Claims by date				✓
Claims edited	✓	✓	✓	
Claims exceptions by reason code	✓	✓	✓	✓
Claims on hold	✓	✓		✓
Claims resubmitted	✓	✓	✓	
Claims submitted, denied	✓	✓	✓	
Claims submitted, paid				✓
Claims voided	✓	✓	✓	
Direct care giver schedule				✓
Prior Authorization, no scheduled visits			✓	
Provider ID does not equal authorized provider ID	✓	✓	✓	
Recipient address change	✓	✓	✓	✓
Recipient list				✓
Visits delivered, deviate from prior authorization		✓	✓	
Visits delivered, start address does not equal end address	✓	✓		✓
Visits late			✓	✓
Visits overlapping services	✓	✓	✓	✓
Visits scheduled	✓	✓	✓	✓
Visits scheduled address does not equal delivery address	✓	✓		✓
Visits scheduled, conflicting prior authorizations	✓	✓	✓	✓
Visits scheduled, no prior authorization		✓	✓	
Visits scheduled, not completed (missed)	✓	✓	✓	✓
Visits supported by third party EVV	✓	✓	✓	✓
Visits unable to complete	✓	✓	✓	

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.

Yes, each user has an online listing with a link to each on-demand report.

DQ023	4587	1	The solution should identify and use consistent report fields.

Yes, Tellus maintains a standard data dictionary across reports, and allows for the application of "skins" to reports to allow for changes in terminology between state Medicaid systems. As an example, Tellus user interfaces and reports can be configured to refer to a recipient as recipient, member, patient, etc.

DQ024	4586	1	The solution should display a consistent format on all reports.

Yes, all Tells reports comply to the Tellus brand guide, giving them a consistent layout and look/feel.

DQ025	4597	1	The solution should have the ability to categorize and organize reports including, but not limited to, the following parameters:
DQ026	4990	2	Source system
DQ027	4991	2	Data content
DQ028	4992	2	Purpose
DQ029	4993	2	Frequency

The system does not categorize reports as described above per se, but reports are presented to applicable users in a well-organized and easy to understand organization.

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:
DQ031	5095	2	Manual edits
DQ032	5096	2	Error corrections
DQ033	5097	2	Additions to the interface records

When performing data interchange, Tellus always:

1. Returns an accepted/rejected response for every inbound transaction.
2. Transmits an accepted/rejected count email to the sender.
3. Processes accepted/rejected response from transmitter for every outbound transaction.
4. Resend rejected outbound records.
5. Displays accepted/rejected status to end users via the user interface when applicable.
6. Generates reconciliation reports for review with data interchange partner.

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.

Tellus EVV runs real time validation checks and business rules throughout the application beginning at the point of data entry. Users are alerted as errors are identified.

Tellus can generate a summary report on a periodic basis and as requested to identify all records requiring remediation. Eligible users will be able to run the report and it will also be provided to DHHR in the method requested.

DQ035	4584	1	The solution should store reports to allow users the ability to retrieve them quickly per the Department's business rules.

Tellus will archive all reports and other documents per agreed-upon data retention requirements.

DQ036	4779	1	The solution should reload or resend records if they have not been applied correctly to the receiving entity.

Tellus EVV can reload or resend records that are not applied correctly by the receiving entity.

DQ037	4780	1	The solution should detect duplicate files or records and isolate them for manual review and further processing.

Tellus EVV is designed to prevent duplicate files or records; however, if duplicates are created, they will be detected and isolated for manual review and further processing.

DQ038	4782	1	The solution should create messages that accurately describe errors received as a result of a data transfer.

When performing data interchange, Tellus always:

1. Returns an accepted/rejected response for every inbound transaction.
2. Transmits an accepted/rejected count email to the sender.
3. Processes accepted/rejected response from transmitter for every outbound transaction.
4. Resend rejected outbound records.
5. Displays accepted/rejected status to end users via the user interface when applicable.
6. Generates reconciliation reports for review with data interchange partner.

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.

Online specifications are available for all web forms.

DQ040	4492	1	The solution should have the ability to identify which fields in forms are required and which are optional.

All web forms are implemented with business rules for required and optional/conditional fields.

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.

Any date/time field can be expressed in any common format.

DQ042	4545	1	The solution should provide automatic default file naming convention for saved correspondence as agreed upon with the Department.

Tellus publishes our default file naming convention, example here:
https://tellusolutions.atlassian.net/wiki/spaces/EVV/pages/487358465/File+Naming+Convention

DQ043	4553	1	The solution should categorize and classify types of correspondence as agreed upon with the Department.

Agreed.

DQ044	4710	1	The solution should distinguish between, and incorporate, business days, weekends, and state holidays in all time-related functions in the system.

The solution does differentiate between weekends and days of the week, but the EVV system is operational 365 days a year, so the differentiation of holidays not been a requirement in the past. If there is a need to differentiate then Tellus will implement a solution to do so.

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.

Tellus offers both inline help and a training/help portal.

DQ046	4472	1	The solution should set parameters on fields to prevent system users from entering information outside of those parameters.

All web forms include automatic validation of all data entry to include required fields, optional conditional fields, and other rules such as field length, data type, whether special characters allowed, etc.

DQ047	4474	1	The Vendor should produce all member- and provider-facing content written at no greater than an eighth-grade reading level.

Our EVV system and training is available in English and Spanish and is written to be understandable by individuals with a reading level equivalent of no greater than eighth grade.

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.

4 HARDWARE AND INFRASTRUCTURE

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.

We recommend one of the two most economical methods of EVV:

- Bring Your Own Device (BYOD), Mobile GPS-Enabled EVV, or
- IVR EVV for all recipients who have a landline at their primary service location address

If the recipient and direct care provider do not have access to a personal smart device or landline, DHHR may consider issuing a small alternative or fixed object device; however, these options are a more expensive alternative. Based on our experience, a BYOD approach will meet the needs of the population being served. If the State prefers to offer an alternative, those services are available at an additional per-device charge.

Tellus EVV works in offline mode for individuals who live in rural areas without reliable cellular, Wi-Fi or GPS services. The provider uses the app as normal. Once they return to Wi-Fi or cellular service again, the data syncs to the system.

The State can also elect to allow IVR for EVV using the Recipient's phone number of records. Toll-free numbers are provided for caregivers to clock-in/clock-out with confirmation of services and tasks rendered during the visit. If a caregiver calls from a telephone number that does not match the Recipient's phone number of records, the mismatch is recorded and reported. Tellus also supports Small Alternative Device (SAD) or Fixed Object (FOB) devices. A random number is generated on the device that the caregiver calls to verify.

Tellus is committed to ensuring our technology remains compliant with all current and future Federal guidelines. Updated releases will be made available at no additional charge.

IN002	4763	1	The Vendor should utilize open architecture standards and scalability to promote integration throughout the West Virginia technology enterprise.

Tellus software is designed as stateless applications improving scalability and interoperability. Caching will be used only when necessary and not detrimental to application usability. As another best practice, all variable parameters are externalized and stored as configuration settings. The system allows different sets of parameters for production, QA and development environments. The applications load parameters from the configuration settings at startup.

The EVV platform is hosted on Amazon Web Services (AWS) Government Cloud and runs on 15 AWS data centers located in the continental U.S.

We use AWS Elastic Load Balancing to automatically route traffic across multiple instances and multiple availability zones. Elastic Load Balancing ensures only healthy Amazon application server instances receive traffic by detecting unhealthy instances and rerouting to healthy servers. If additional computing capacity is required, we have systems in place to scale the application and database service layers to ensure SLAs are met.

AWS CloudWatch is used to monitor network traffic, bandwidth usage and bottlenecks that impede performance. Monitoring and auto-scaling systems provide the information required to diagnose system performance issues, errors and backlogs. Monitoring includes, but is not limited to, CPU, memory utilization, network and disk utilization. For the database server, we also monitor read/write latency, number of sessions and session performance. Our engineers get immediate notifications about all system issues. If these cannot be resolved immediately, notifications will be forwarded to the State and/or Providers as required based on service level agreements.

IN003	4758	1	The solution should be flexible and readily adaptable to changing Department and federal requirements and as requested by the Department.

We use AWS Elastic Load Balancing to automatically route traffic across multiple instances and multiple availability zones. Elastic Load Balancing ensures only healthy Amazon application server instances receive traffic by detecting unhealthy instances and rerouting to healthy servers. If additional computing capacity is required, we have systems in place to scale the application and database service layers to ensure SLAs are met.

Using Amazon RDS allows us to scale database's compute and storage resources within minutes, often with no downtime. We are able to launch one or more Read Replicas to offload read traffic from primary database instance.

Tellus is committed to ensuring our technology remains compliant with all current and future Federal guidelines. Updated releases will be made available at no additional charge.

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.

The EVV platform is hosted on Amazon Web Services (AWS) Government Cloud and runs on 15 AWS data centers located in the continental U.S. AWS datacenters are distributed in geographic regions that include clusters of datacenters called Availability Zones. Every region is geographically isolated in terms of power and water supply, and each zone is similarly served by independent networks. Redundantly storing information in different datacenters in multiple regions, availability zones and datacenters greatly reduces downtime, as the nearest available node is activated as a backup

In case of failure of the primary node, Amazon RDS performs an automatic failover to the standby without the need for manual intervention. Within minutes, a new instance of the server is launched in a different AWS availability zone or region. Downtime is cut to minutes instead of hours. Using various AWS regions and different physical data centers ensures the system is highly available and fault tolerant.

The server environment is virtualized. This allows for portability in case the disaster affects the datacenter when the application server is running. Within minutes, a new instance of the same server will be launched in a different datacenter in a different AWS availability zone or region. As mentioned, this cuts downtime to minutes.

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.

Tellus EVV works in offline mode for individuals who live in rural areas without reliable cellular, Wi-Fi or GPS services. The provider uses the app as normal. Once they return to Wi-Fi or cellular service again, the data syncs to the system.

As long as the direct care provider opens the EVV app on their mobile device while they

have access to Wi-Fi or cellular service, their schedule will sync to the mobile device. All service data can be captured and cached whether or not the direct care provider has network connectivity. All data is encrypted at rest and in transit. When the direct care provider regains Wi-Fi or cellular service, all activity captured while the mobile device was in offline mode is automatically synced to the EVV database.

This feature provides the ability to capture electronically verified visit information even for recipients who live in areas with limited wireless network connectivity. GPS trilateration is used to capture coordinates even when Wi-Fi and cellular service is unavailable.

IN004	4725	1	The solution should provide archival and purge processes that do not degrade performance or interrupt the system.

All processes that load the database are run either on a read-replica database or run during maintenance windows overnight.

IN005	4748	1	The solution should allow centralized deployment of system updates and system maintenance.

Tellus uses a formalized SCM process with Git as a source repository, Jenkins, Flyway, and Kubernetes for orchestration, and a Docker container system.

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:
IN007	5090	2	Communication events (email, document upload, form submissions, or phone)
IN008	5091	2	System-generated events
IN009	5092	2	User-triggered events
IN010	5093	2	Exception-processing events

Yes, Tellus EVV supports these triggering events.

IN011	4673	1	The solution should include definition and modeling of workflow processes and their constituent activities.

Tellus EVV workflows are defined and modelled most typically using UML sequence and data flow diagrams.

IN012	4529	1	The solution should have the ability to facilitate mass email notifications.

The solution includes support for mass email and mass SMS notifications.

IN013	4533	1	The solution should have the ability to reissue and track any correspondence or form as requested by the Department.

The Tellus EVV solution includes a messaging infrastructure that allows for communications to be:

1. Triggered by any of a number of processes, including missed events, user interface activity, business events such as PA status.
2. Transmitted to one or multiple mobile and or web portal users or user roles via email, browser page inbox, or SMS.
3. Track whether viewed.
4. Long-term archived per data retention policies.

IN014	4565	1	The solution should have the ability to schedule any report to be run at varying levels of frequency or on-demand.

All reports can be run on a schedule or on demand. Schedule frequencies can vary.

IN015	4576	1	The solution should provide integrated print capability within the application for any report.

All reports can be downloaded and/or printed directly from the EVV solution.

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.

Tellus currently utilizes both web banners and individual emails to notify users of system maintenance and other information approved to be distributed by the Department. Often, join communication is found to be useful from both the Department and Tellus.

The Tellus product roadmap includes a "provider message board" function that will allow for the Department to communicate with providers and fiscal agents. This functionality will be in production in time for the Department implementation.

IN017	4400	1	The Vendor should manage, track, and report on user support services via multiple channels, including.
IN018	4401	2	Telephone
IN019	4402	2	Member portal
IN020	4403	2	Email
IN021	4404	2	Mail

Yes, the Tellus contact center manages, tracks and reports on support services via multiple channels including phone, web portal, chat, email and mail upon request. All contacts are documented in our ZohoDesk ticketing system, and reporting on user support metrics is provided monthly or upon request.

IN022	5215	1	The Vendor should provide investigative results inclusive of mitigation measures to address reported incidents within 30 days of the documented incident.

Our project management approach includes testing at key checkpoints in the overall process to determine whether objectives are being met. Testing operations are planned, managed and executed in every phase of the project to cover unit, system, regression, parallel, integration, and user acceptance testing.

JIRA is one of the tools used for the tracking of operations and as the common repository of testing information, including testing artifacts such as test cases and test results. Each resource in the Testing team is provided with Read/Write access to add/modify test cases. During the Test Design phase, all test cases are written directly into JIRA. Any change to the test case is directly saved and logged.

Throughout testing, each tester directly accesses their respective assigned test cases and updates the status of each executed step. Any defect encountered is logged, linking to the particular test case/test step. During Defect fix testing, defects are re-assigned back to the tester to verify the defect fix. The tester verifies the defect fix and updates the status directly in JIRA. Reports are routinely created by our testing team and project managers to provide updates on the status of test execution. For example, these reports may include a status report of test cases executed.

To ensure application functionality and 24/7 uptime, we adhere to the following service level and system problem plan:

- Application defects will begin with a diagnosis and classification of the reported issue within one (1) hour of Tellus being alerted or identified by Tellus.
- Application defects identified as Severity 1 will begin the resolution process within four (4) hours of identification.
- Application defects identified as Severity 2 will begin the resolution within one (1) business day and scheduled for emergency release.
- Application defects identified as Severity 3 will begin resolution within five (5) business days and added to the next scheduled release. Service Level Agreement (SLA) definitions will be outlined during the contracting process, examples may include:

Application Defect – A defect is defined as an error, flaw, failure or fault within the Tellus EVV platform.

- Severity 1 – An application defect is deemed Severity 1 when the majority of services are not available for use by the end users. This includes internal users of the system.
- Severity 2 – An application defect is deemed Severity 2 when a portion of services are not available for use by the end users or an intermittent failure is occurring with seemingly random sequences of events. This includes internal users of the system.
- Severity 3 – An application defect is deemed Severity 3 when there is an isolated issue pertaining to an individual or small group of users that have impact on their ability to use the system. This includes internal users, items initially reported as defects but later classified as enhancements, and issues reported that are unable to be replicated by reasonable means. Severity 3 defects will be reported on regularly and reviewed for larger patterns. A group of Severity 3 defects may potentially escalate in severity classification if patterns are identified that indicate a larger problem.

Tellus will provide detailed incident resolution reports to the DHHR, including root cause corrective action. Incident resolution reports will be provided within five (5) business days of resolution of the incident.

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.

We provide comprehensive training and outreach to support the Tellus EVV solution at implementation and beyond. Our training platform and modules are designed to address the needs of each unique audience. They are also compliant with the Americans with Disabilities Act supporting alternative delivery mechanisms for the greatest degree of accessibility for Recipients and Providers with a wide range of disabilities. Our materials are written in a non-technical, easy-to-understand manner with simple step-by-step instructions and visual cues. We offer a multi-modal approach to training.

Tellus EVV also includes a comprehensive online training and support center that serves as a central repository for all learning materials. It houses the training calendar where individuals can register for upcoming, hands-on training courses. It also offers detailed user manuals, FAQs, video tutorials, recorded courses for self-paced learning as well as other essential learning tools and reference guides. The center is organized in a simple,

straightforward fashion, making it easy for individuals to quickly access the content that's relevant to them.

In addition, we use a complaint resolution, customer service and tracking system that identifies and tracks provider calls into our help desk. The help desk is located in Boca Raton, FL, where customer requests are taken by reps supported by an interactive voice response system, computers, headsets and software to distribute calls and collect data. Our primary goal is to ensure customer service satisfaction.

The help desk is accessed by a U.S.-based toll-free number that's operational 24/7. Our help desk is supported by English and Spanish speaking staff. Our trained customer service reps are available during normal business hours defined as 8 a.m. to 5 p.m. Eastern Monday through Friday, excluding major holidays.

During normal business hours the customer service phone number is initially answered by an interactive voice response system giving callers the option to speak to a live person in either English or Spanish. There is a mechanism to assist people with hearing or speech disabilities. Ninety percent (90%) of calls are answered within thirty (30) seconds with only ten percent (10%) requiring a message be left. All voice mail messages received during normal business hours are returned within one (1) hour.

Outside of normal business hours, the interactive voice response system will inform callers of the help desk hours of operation and provide them the option to leave a message. Callers leaving messages will be called back the next business day.

All inquiries and complaints are resolved as soon as possible but no later than an average of ten business days from initial receipt. Inquires and complaints and the resulting resolution are tracked using an internal ticketing system that records the initial complaint/inquiry including caller identification, time, date, message, steps taken to remediate the information conveyed and the final resolution. If procedural changes are required as the result of any complaint, this information is documented and provided to the State as part of our quarterly report. Procedural changes will be formally written, dated and communicated to all relevant parties.

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.

See hardware & software requirements:

https://tellusolutions.atlassian.net/wiki/spaces/EVV/pages/662405167/Minimum+Hardware+and+Software+Requirements

IN025	4499	1	The solution should allow users to schedule and modify system events as requested by the Department.

Tellus will coordinate with the department to coordinate the scheduling of system events, most notably the timing of data interchange processing.

IN026	4408	1	The Vendor should provide a technical support call center located within the contiguous United States.

The Tellus Customer Success Team (support center) is located in Boca Raton, FL, where customer requests are taken by representatives supported by an interactive voice response system, computers, headsets and software to distribute calls and collect data. Our primary goal is to ensure customer service satisfaction.

IN027	4450	1	The solution should document call information, as agreed upon by the Department.

Inquires and complaints and the resulting resolution are tracked using an internal ticketing system that records the initial complaint/inquiry including caller identification, time, date, message, classification of issue, steps taken to remediate the information conveyed and the final resolution. If procedural changes are required as the result of any complaint, this information is documented and provided to the State as part of our quarterly report. Procedural changes will be formally written, dated and communicated to all relevant parties.

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,

The help desk is accessed by a U.S.-based toll-free number that's operational 24/7. Our help desk is supported by English and Spanish speaking staff. Our trained customer service reps are available during normal business hours defined as 9 a.m. to 6 p.m. Eastern Monday through Friday, excluding major holidays. When requested by the Department, additional call center hours of operation will be made available.

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

Outside of normal business hours – 9 a.m. to 6 p.m. Eastern Monday through Friday, excluding major holidays – the interactive voice response system will inform callers of the help desk hours of operation and provide them the option to leave a message. Callers leaving messages will be called back the next business day in the caller's preferred language and/or through oral interpretation services.

IN030	4415	1	The Vendor should provide functionality to manage calls to the Technical Call Center including, but not limited to:
IN031	4922	2	Creation of tickets
IN032	4923	2	Editing existing tickets
IN033	4924	2	Sorting of call center ticket information
IN034	4925	2	Filtering of call center tickets or electronic records

We use a complaint resolution, customer service and tracking system that identifies and tracks all contacts into our help desk, including mail, email, web, chat and telephone.

Inquires and complaints and the resulting resolution are tracked using an internal ticketing system that records the initial complaint/inquiry including caller identification, Vendor staff responding to the ticket or having contributed to the resolution of the ticket, time, date, message/initial concern, classification of issue, steps taken to remediate the information conveyed and the final resolution (status). If procedural changes are required as the result of any complaint, this information is documented and provided to the State as part of our quarterly report. Procedural changes will be formally written, dated and communicated to all relevant parties.

Tickets may be edited, and a full audit log is included of all notes made within the ticket and routing for resolution, including time, date and Vendor staff name/s. This information can be sorted and/or filtered in various ways including but not limited to CSR name, date, time, provider name, status, high-level classification of issue and resolution time.

IN035	4416	1	The Vendor's Technical Call Center should have the ability to track data including, but not limited to:
IN036	4417	2	The caller
IN037	4418	2	The question(s) and/or issue(s)
IN038	4419	2	The Vendor staff responding to the ticket
IN039	4420	2	The date(s)
IN040	4421	2	The time(s)
IN041	4422	2	The status (opened or closed)
IN042	5217	2	Problem resolution

Inquires/issues and the resulting resolution are tracked using an internal ticketing system that records the initial complaint/inquiry including caller identification, Vendor staff responding to the ticket or having contributed to the resolution of the ticket, time, date, message/initial concern, classification of issue, steps taken to remediate the information conveyed and the current and final resolution (status). If procedural changes are required

as the result of any complaint, this information is documented and provided to the State as part of our quarterly report. Procedural changes will be formally written, dated and communicated to all relevant parties.

IN043	4431	1	The Vendor's Technical Call Center should have the ability to repeat call options automatically.

The Tellus Client Success Team/Contact center has the ability to repeat call options automatically in addition to other features including immediately opting to leave a voice mail message for a call back, the identification of how the long the wait queue is/what # in line they are for the next agent to be available and other useful features.

IN044	4437	1	The Vendor should maintain sufficient staff and telephone lines to perform all required technical support call center functions.

Workforce planning is in place to identify the number of staff to perform all required technical support call center/contact center functions. Voice Over Internet Protocol (VOIP) ensures that there is no limit to the number of "telephone lines" that are available for contacting Tellus.

IN045	4798	1	The solution should use automated menus, including an easily accessible option for reaching a live operator.

During normal business hours the customer service phone number is initially answered by an interactive voice response system giving callers the option to speak to a live person in either English or Spanish. Automated menus are in use, and can be customized for this program, including recording of answers to commonly asked questions that can be resolved without having to wait for a live operator for resolution (common examples are "where do I go to register for a training session" or "how do I reset my password). Our AWS Connect solution is easily customizable for reaching a live operator upon request.

IN046	4901	1	The solution should provide assistance to inquiries received from persons who require special assistance including, but not limited to:
IN047	5031	2	Persons with Limited English Proficiency (LEP)
IN048	5032	2	Persons with vision disabilities
IN049	5033	2	Persons with hearing disabilities
IN050	5034	2	Persons with speech disabilities

Our help desk is supported by English and Spanish speaking staff. During normal business hours the customer service phone number is initially answered by an interactive voice response system giving callers the option to speak to a live person in either English or Spanish. There is a mechanism to assist people with hearing or speech disabilities, as well as those with Limited English Proficiency.

IN051	4885	1	The solution should include an online option for users to report any technical problems.

The Tellus EVV solution includes an online option for users to report any technical problems through a feature on our web page. Additionally, a chat feature is often made available throughout the day for those that wish to receive chat support.

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:
IN053	5191	2	Microsoft Edge
IN054	5192	2	Apple Safari
IN055	5193	2	Google Chrome

IN056	5194	2	Mozilla Firefox
IN057	5195	2	Microsoft Internet Explorer

The EVV platform is an AWS Government Cloud-hosted solution. This greatly facilitates rapid system deployment for DHHR and provides access to all stakeholders to required functionality through free, widely used web browsers and native mobile apps. Tellus certifies support for the EVV Console (browser-based), Claims Console (browser-based) and EVV Mobile App (mobile device app) on the following:

See hardware & software requirements:

https://tellusolutions.atlassian.net/wiki/spaces/EVV/pages/662405167/Minimum+Hardware+and+Software+Requirements

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.

All portal and mobile apps have a shallow navigational structure, with easy 1- or 2-click access to all menus.

IN059	4820	1	The solution should generate drop-down lists to identify options available, valid values, and code descriptions by screen field.

Yes, the system features a database type code catalogue that allows for the easy implementation and maintenance of drop-down lists.

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.

Tellus provides web applications that satisfy the Priority 1 Checkpoints as listed above.

IN061	4838	1	The solution should have the ability to include secure and public facing tabs for the web portal.

Yes, while most pages require login to access, the system supports anonymous access to public information.

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.

Access to the EVV solution is tightly controlled using secure login ID and device access controls. System security is integrated into the system's basic design. We have a number of standard security features to make sure that only authorized users can access the system and its data, including user authentication through IDs and passwords, functional access controls, multiple firewalls and several different virus protection products. Data transmitted between external systems and our servers are protected by authentication and encryption, while secure file transfer protocols (SFTP) are always used for data file transmissions.

The EVV data collection mobile app is easily loaded onto devices used to capture EVV data. The app can be downloaded from commercially available app stores onto any smart Android or iOS device meeting minimal requirements. The device is associated with the user with valid login credentials, a login ID and password. Recipient data cannot be accessed without secure login credentials and the creation of a schedule linking a recipient to a direct care provider. The schedule must be created by an administrative user associated with a provider or fiscal intermediary. The criteria to create multiple layers of authentication will include:

- User must be created with secure login credentials providing a cell phone or email address.
- User must be associated with a member by an administrator associated with a provider or fiscal intermediary.
- User must log in to mobile app to start and end visit. GPS functionality must be enabled on the mobile app at the beginning and end of the visit for GPS coordinates to be captured.

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.

Both the web-based consoles and mobile app have options where users can request a password reset. They will receive an email that requires a timed response in order to create a new password. Users can also contact their system administrator for a password reset.

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.

Passwords can be hidden and revealed by users only on the mobile app. On the web-based portal, passwords are always hidden.

IN065	4882	1	The Vendor should ensure that web portal field definitions comply with system field definitions.

Yes, the system is aligned between dataset, microservice layer, and presentation layer.

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).

Tellus IT security is comprised of an interlocking wall of infrastructure, defensive technology, monitoring technology, training, process, and procedures. Tellus will self-certify for HITRUST (including HITECH and GovRamp) in 2019.

The Tellus EVV web application and API deliver information through both public and private interfaces. Data security is managed through various protocols and user authentication and authorization. Secure Sockets Layer (SSL) encryption is the standard for communications over the Internet. When configured to use SSL, the application enforces secure communications in all private areas of the website by disallowing non-secure HTTP requests and redirecting the browser to the secure protocol.

Database security begins with hardened, redundant Amazon Government Cloud (AWS) database servers. AWS is a top-tier, SAS 70 Type II certified datacenter. The database and application are configured in separate tiers of the physical systems, with strict firewall rules partitioning the servers.

The EVV platform is hosted on Amazon Web Services (AWS) Government Cloud and runs on 15 AWS data centers located in the continental US. AWS datacenters are distributed in geographic regions which include clusters of datacenters called Availability Zones. Every region is geographically isolated in terms of power and water supply, and each zone is similarly served by independent networks. Redundantly storing information in different datacenters in multiple regions, availability zones, and datacenters greatly reduces downtime, as the nearest available node is activated as a backup.

Each AWS datacenter is protected by four distinct layers of security:

- **Perimeter Layer** - Datacenters are physically enclosed by gates protected by security guards and intrusion detection technology
- **Infrastructure Layer-** Energy generators, fire suppression equipment, and ordinary and extraordinary maintenance systems protect the integrity of the data stored in the datacenter
- **Data Layer-** Access to server rooms is restricted, tightly regulated by authorization processes and constantly monitored
- **Environmental Layer-** The locations where AWS datacenters are built are screened for seismic activity and extreme weather, to minimize the risk of structural damage caused by natural occurrences

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.

All PHI data is encrypted in transit and at rest when stored in a database or filesystem. We use Transparent Data Encryption (TDE) and adhere to HIPAA compliance.

The process of retrieving visit verifications in compliance with HIPAA standards requires all communications (application <--> database, mobile app > server) happen over a secure HTTPS connection. We ensure that PHI information is encrypted when transmitted and encrypted at rest by using SSL/TLS and database encryption. Our hosting provider has achieved a number of certifications including, but not limited to, SOC 1,2,3, FedRAMP, ISO 9001, HITECH, PCI DSS: (https://aws.amazon.com/compliance/)

5 SECURITY MANAGEMENT

SM001	4230	1	The solution should authenticate all users when establishing a connection to the solution.

Access to the EVV solution is tightly controlled using secure login ID and device access controls. System security is integrated into the system's basic design. We have a number of standard security features to make sure that only authorized users can access the system and its data, including user authentication through IDs and passwords, functional access controls, multiple firewalls and several different virus protection products. Data transmitted between external systems and our servers are protected by authentication and encryption, while secure file transfer protocols (SFTP) are always used for data file transmissions.

The EVV data collection mobile app is easily loaded onto devices used to capture EVV data. The app can be downloaded from commercially available app stores onto any smart Android or iOS device meeting minimal requirements. The device is associated with the user with valid login credentials, a login ID and password. Recipient data cannot be accessed without secure login credentials and the creation of a schedule linking a recipient to a direct care provider. The schedule must be created by an administrative user associated with a provider or fiscal intermediary. The criteria to create multiple layers of authentication will include:

- User must be created with secure login credentials providing a cell phone or email address.

- User must be associated with a member by an administrator associated with a provider or fiscal intermediary.
- User must log in to mobile app to start and end visit. GPS functionality must be enabled on the mobile app at the beginning and end of the visit for GPS coordinates to be captured.

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.

SM003	3975	1	The solution should have the ability to assign a new unique user identifier (ID) for an existing user.

Each user record is automatically created with a GUID as the primary database identifier.

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.

Data transmitted between external systems and our servers are protected by authentication and encryption, while secure file transfer protocols (SFTP) are always used for data file transmissions.

All PHI data is encrypted in transit and at rest when stored in a database or filesystem. We use Transparent Data Encryption (TDE) and adhere to HIPAA compliance.

The process of retrieving visit verifications in compliance with HIPAA standards requires all communications (application <--> database, mobile app > server) happen over a secure HTTPS connection. We ensure that PHI information is encrypted when transmitted and

encrypted at rest by using SSL/TLS and database encryption. Our hosting provider has achieved a number of certifications including, but not limited to, SOC 1,2,3, FedRAMP, ISO 9001, HITECH, PCI DSS: (https://aws.amazon.com/compliance/)

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.

The system currently contains similar warnings for download of PHI and can be enhanced with warnings as required by the Department.

SM006	4244	1	The Vendor should provide a secure web-based method to receive requests for authorization to access the solution.

Role-based account permissions are used to provide native user authentication based on account name, username and a user-supplied password. User password is stored in the database and hashed using one-way BCrypt hashing mechanism that makes it impossible to decrypt and extremely resistant to brute-force search attacks

SM007	4246	1	The Vendor should provide Single Sign-On (SSO) capability for authentication and authorization across the solution.

Tellus assigns a unique database identifier as a GUID to each user record, this allows for other identifiers such as Medicaid ID, email, login user ID, etc. to be updated as necessary.

SM008	4254	1	The solution should provide Department-approved multi-factor authentication for Vendor remote access to solution environment or their contractors, if applicable.

Tellus supports MFA to the extent that is supported by the accessing device (smart phone, browser, etc.)

SM009	3977	1	The solution should use role-based access for data and system functionality.

Access to components of the application and the ability to view and write to specific fields is controlled by secure, private login credentials as well as by role-based permissions. User roles are defined during the business requirements gathering phase of the project.

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.

Business rules are generally defined by payer. However, they can be created at any level, using the following hierarchy:

- Jurisdiction (State)
- Payer
- Plan
- Program
- Provider
- Caregiver
- Recipient

This classification system enables DHHR to configure the EVV application at the program level. Program rules, services, policies and procedures and reimbursement rates can be defined at the program/provider level. Business rules can also be written based on these categories as well as at the field level. Because our business rules engine is a module independent of the software code base, rules can be changed during the term of the contract without the use of development resources, providing maximum flexibility.

User-based permissions, combined with flexible rules, allow the ability to customize user privileges by program. That means a provider can be granted the right to enter service tasks on one program by personnel type and not have that same access for another program.

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:
SM012	5043	2	Username
SM013	5044	2	Date of access
SM014	5045	2	Time of access
SM015	5046	2	Name of Individual (First and Last) whose confidential personal information (CPI) was accessed
SM016	5047	2	Name of computer system used to access confidential personal information (CPI)
SM017	5048	2	Query/Transaction used

Yes, the solution logs this information with the exception of computer name—it instead logs IP address.

SM018	4082	1	The solution should provide users role-based access to reporting functionality.

Access to reports and reporting tools is granted based on user role permissions.

SM019	5218	1	The solution should allow correspondence to be viewed based on role-based access.

Yes, all reports and documents are controlled by role-based and/or individual user-base access.

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.

Yes, the solution supports a read-only indicator that can be set on any user role.

SM021	4229	1	The solution should provide role-based security through various methods, including, but not limited to:
SM022	5052	2	Unique identifiers (IDs)
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
SM024	5054	2	Profile or group access assignments

SM025	4235	1	The solution should provide a mechanism to limit access to information based on user roles and program rules.

Access to components of the application and the ability to view and write to specific fields is controlled by secure, private login credentials as well as by role-based permissions. User roles are defined during the business requirements gathering phase of the project. Examples of roles are:

Module Access	User Role	View Data	Enter/Modify Data
Mobile App	Direct Caregiver	Yes, for Scheduled Visits	Yes, for Scheduled Visits
Mobile App	All Other User Roles	No	No
Provider Administration	Provider Administrator	Yes	Yes
Provider Administration	All Other User Roles	No	No
Provider Scheduling	Provider Scheduler	Yes	Yes
Provider Scheduling	Provider Administrator	Yes	Yes
Provider Scheduling	All Other User Roles	No	No
Claims Processing	Provider Claims Processor	Yes	Yes
Claims Processing	Provider Administrator	Yes	Yes
Claims Processing	All Other User Roles	No	No
Provider Reporting	Provider Administrator	Yes	Yes
Provider Reporting	Provider Scheduler	Yes, Visit Reports	No
Provider Reporting	Provider Claims Processor	Yes, All Reports	No
Provider Reporting	Case Manager	Yes, All Reports for Assigned Recipients	No
Provider Reporting	Program Manager	Yes, All Reports for Assigned Programs	No

Provider Reporting	Payer Administrator	Yes, All Reports for Assigned Programs	No

These examples are not exhaustive; they are simply a representation of potential roles that can be defined.

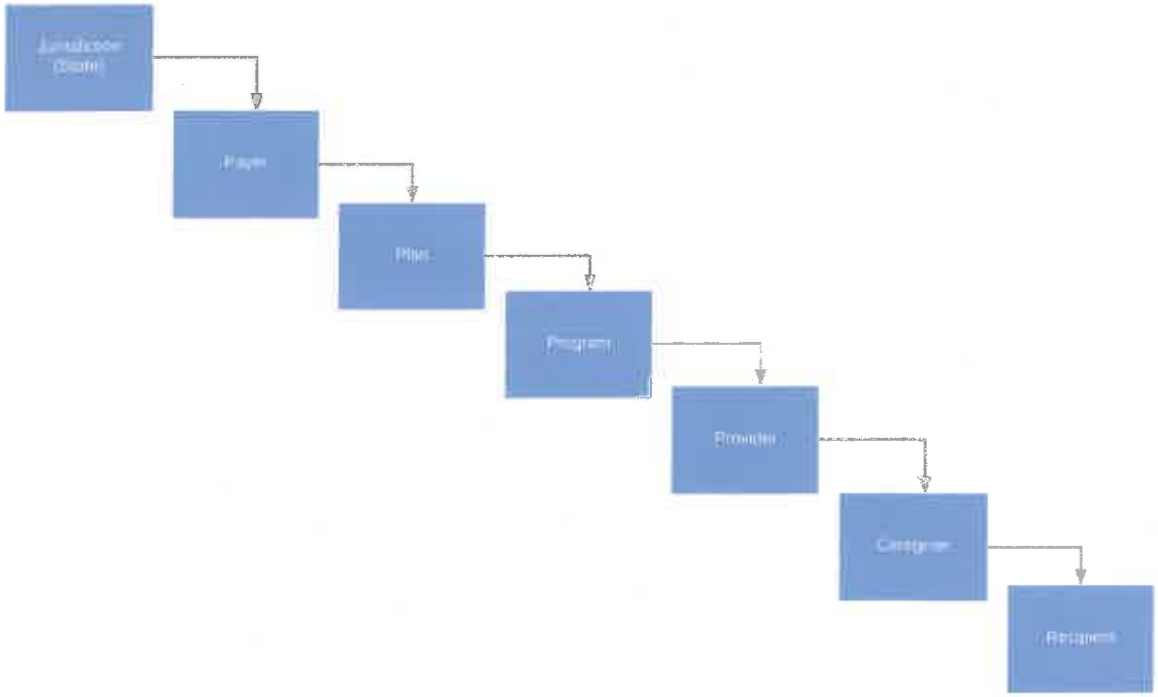
In summary, access can be granted at the Module level. The ability to view data can be restricted at the field level so a Provider Scheduler may be able to view some components of the Recipient record like name, phone number, address and services to be rendered. However, Medicaid ID can be hidden from view.

In addition, the ability to Enter/Modify data can be restricted by role. As an example, the Recipient Address of record can only be changed by a Payer data feed, but alternative addresses can be added by the Provider Administrator and the Scheduler.

Another example is associating tasks with service codes. If the State authorizes providers to add and edit tasks, the Provider Administrator may be given permission to add tasks to service codes. If the State wants tasks defined at the program level, the Provider Administrator will not be given permission to add tasks to service codes. That privilege will be retained by the Program Manager.

Tellus EVV is multi-tiered with access defined by user roles. Providers can only see data related to their Agency. Payers can view data for all the Providers in their network

In addition, data is categorized using the hierarchy depicted below:



For the State, this means prior authorizations will be categorized by program, so if recipient Jane Doe receives personal care services under multiple programs: State Plan, EPD Waiver and IDD Waiver, the prior authorization for each program will be categorized by that program and only the Provider for that specific program will be aware of that prior authorization.

For example, if Jane Doe receives services under the State Plan by Caring Angels and services under the EPD Waiver by Helping Hands, the prior authorization issued by the State Plan will be available for Caring Angels to deliver services under the State Plan but Helping Hands will not know that this prior authorization was issued. Segregating data by program provides the ability to create user-based roles and permissions that protect private health information by allowing only users who need access to specific information view it. User-based roles and permissions are set for both viewing and modifying data.

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:
SM027	5055	2	Blocking specific window or screen access
SM028	5056	2	Blocking specific report views or analytics
SM029	5057	2	Restrict data elements
SM030	5058	2	Restrict viewing of specific members
SM031	5059	2	Limit access to other fields within the system as determined by the Department

Access to components of the application and the ability to view and write to specific fields is controlled by secure, private login credentials as well as by role-based permissions. User roles are defined during the business requirements gathering phase of the project. Examples of roles are:

Module Access	User Role	View Data	Enter/Modify Data
Mobile App	Direct Caregiver	Yes, for Scheduled Visits	Yes, for Scheduled Visits
Mobile App	All Other User Roles	No	No
Provider Administration	Provider Administrator	Yes	Yes
Provider Administration	All Other User Roles	No	No
Provider Scheduling	Provider Scheduler	Yes	Yes
Provider Scheduling	Provider Administrator	Yes	Yes

Provider Scheduling	All Other User Roles	No	No
Claims Processing	Provider Claims Processor	Yes	Yes
Claims Processing	Provider Administrator	Yes	Yes
Claims Processing	All Other User Roles	No	No
Provider Reporting	Provider Administrator	Yes	Yes
Provider Reporting	Provider Scheduler	Yes, Visit Reports	No
Provider Reporting	Provider Claims Processor	Yes, All Reports	No
Provider Reporting	Case Manager	Yes, All Reports for Assigned Recipients	No
Provider Reporting	Program Manager	Yes, All Reports for Assigned Programs	No
Provider Reporting	Payer Administrator	Yes, All Reports for Assigned Programs	No

These examples are not exhaustive; they are simply a representation of potential roles that can be defined.

In summary, access can be granted at the Module level. The ability to view data can be restricted at the field level so a Provider Scheduler may be able to view some components of the Recipient record like name, phone number, address and services to be rendered. However, Medicaid ID can be hidden from view.

SM032	4237	1	The solution should update all security roles automatically when a change in the master role is made.

Yes, when the privileges for a user role are updated, all users that have that role will automatically be updated real-time.

SM033	4238	1	The solution should allow user access and role changes to be made in real-time.

Yes, changes to role definitions are made through the Tellus internal administrative portal and can be made real-time.

SM034	4240	1	The solution should have the ability to restrict concurrent logons.

A caregiver cannot be logged into more than one visit at a time. If more than one recipient is being treated by one caregiver at the same time, the recipients must be scheduled on the same visit record by an administrator. This is the only mechanism that will allow one caregiver to provider overlapping services with data that is electronically captured using Tellus EVV. It may be necessary for two direct car providers to deliver services to one recipient at the same time. Each care provider is independently scheduled and logged into the visit. Administrators will be able to see the two visits in progress both real time in using reporting tools.

SM035	5167	1	The solution should have the ability to configure the timeout requirements for each system environment and user role.

Timeouts are configurable by application and environment only.

SM036	4204	1	The solution should have the ability to create multi-level escalating alerts for Department-defined events.

Tellus has the ability to create multi-level escalating alerts for specified events.

SM037	4207	1	The solution should identify the recipients of alerts by alert type and user role.

The Tellus EVV solution includes a messaging infrastructure that allows for communications, including user messages and alerts to be:

1. Triggered by any of a number of processes, including missed events, user interface activity, business events such as PA status.
2. Transmitted to one or multiple mobile and or web portal users or user roles via email, browser page inbox, or SMS.
3. Track whether viewed.
4. Long-term archived per data retention policies.

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.

Yes, the system is configurable with a broad catalogue of business rules that will be expanded as part of this implementation. Tellus will coordinate with the Department to define and configure rules as necessary to meet the Department's business requirements.

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:
SM040	5060	2	Alert generation for attempts to access unauthorized databases from internal and external systems
SM041	5061	2	Monitoring and reporting of events on an ongoing basis

Yes, Tellus operates SumoLogic as our SIEM solution for event management.

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:
SM043	5157	2	Non-compliant and required security and privacy controls
SM044	5158	2	Applied mitigations
SM045	5159	2	Plan to correct deficiencies

This information is available as part of our InfoSec package upon request.

SM046	4572	1	The solution should maintain a list of users and owners of each stored report.

This information is available as part of our InfoSec package upon request.

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)

Yes, all system data including reports will be retained per the Department's data retention policy.

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.

Agreed.

SM049	4590	1	The solution should track and store detailed information regarding all reporting requests, including, but not limited to:
SM050	4591	2	Who requested the information
SM051	4592	2	Date of request
SM052	4593	2	Time of request
SM053	4594	2	What data the report included
SM054	4595	2	Report storage upon completion

This information is captured by our BI solution logs and can be made available upon request.

SM055	4757	1	The solution should generate a periodic report of upcoming user account terminations on a schedule approved by the Department.

Yes, this report can be generated.

SM056	4801	1	The solution should maintain a record of all Integrated Eligibility Solution (IES) member information accessed.

The Tellus EVV User Management platform retains a log of all system access.

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.

The Tellus EVV User Management platform retains a log of all system access and all reporting requests.

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.

This information is available as part of our InfoSec package upon request.

SM059	4228	1	The solution should log manual overrides and report on them at timed intervals determined by the Department.

The system captures all manual overrides made to claims as part of unmatched claims remediation and makes this information available via the Payer Portal.

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.

The Tellus EVV User Management platform retains a log of all system access and all reporting requests.

SM061	4281	1	The solution should have the ability to provide authorized requestors a report containing the security profile for an individual or role.

The Tellus EVV credentialing solution maintains a record of all user security profiles.

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.

Yes, this type of reporting is defined via the Tellus Incident Response Policy.

SM063	4301	1	The Vendor should conduct annual penetration testing of the solution and provide results to the Department within 30 days of completion.

Tellus undergoes annual penetration testing and external audits by an independent third party at our major data centers to review performance against identified control objectives and will provide the DHHR with reporting. We will work with the DHHR to remediate any identified vulnerabilities in a mutually agreed upon timeframe. Patching and corrections related to security vulnerabilities of a critical nature will occur within three (3) business days and those of a major nature within ten (10) business days.

Tellus' Security Operations Center (SOC) personnel monitor NIDS sensors 24/7 for security incidents. Tellus' SOC personnel provide Level 1 and 2 supports on security incidents and Security Engineering personnel provide Level 3 support for serious incidents. Tellus leverages Cisco as well as Open Source SNORT and McAfee in our IDS monitoring and reporting solution. For monitoring emerging information security threats and vulnerabilities, Tellus has established and formally documented Incident Response/Crisis Management (IR/CM) policies and procedures .The Incident and Crisis Response Center (ICRC) tracks, documents, and reports security incidents to higher level Tellus officials, and addresses accidental or unauthorized disclosure, modification, or destruction of ePHI or confidential information by technical or non-technical workers (support, janitorial, maintenance, and or vendors), operations staff (IT, managers, etc.), criminal acts, natural disasters, and/or labor strikes.

SM064	4303	1	The Vendor should provide all incident reporting to the Department immediately upon discovery per Department guidelines.

Yes, this type of reporting is defined via the Tellus Incident Response Policy.

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.

The solution does not currently support build-in data redaction functionality.

SM066	4488	1	The solution should allow users to override and change pre-populated information in forms, when appropriate.

Yes, users can update and save information presented in web forms with appropriate. The system will automatically prevent user updated of data that is intended to be read-only per the given user's role.

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)

Tellus EVV will inventory and store all system-generated correspondence based on the BMS Retention Policy.

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)

Tellus EVV stores all data electronically. All data will be retained, stored, imaged, archived and protected from destruction. Data will be made available to DHHR and federal agencies

in accordance with the DHHR Data Retention Policy.

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)

Tellus will archive all hard- and softcopy reports and other documents per agreed-upon data retention requirements.

SM070	4660	1	The solution should prevent certain decisions and fields from having the ability to be overridden by users.

Yes, users can update and save information presented in web forms with appropriate. The system will automatically prevent user updated of data that is intended to be read-only per the given user's role.

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.

Agreed.

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.

Yes, terms of use are enforced via a click-sign agreement upon first portal/app access and

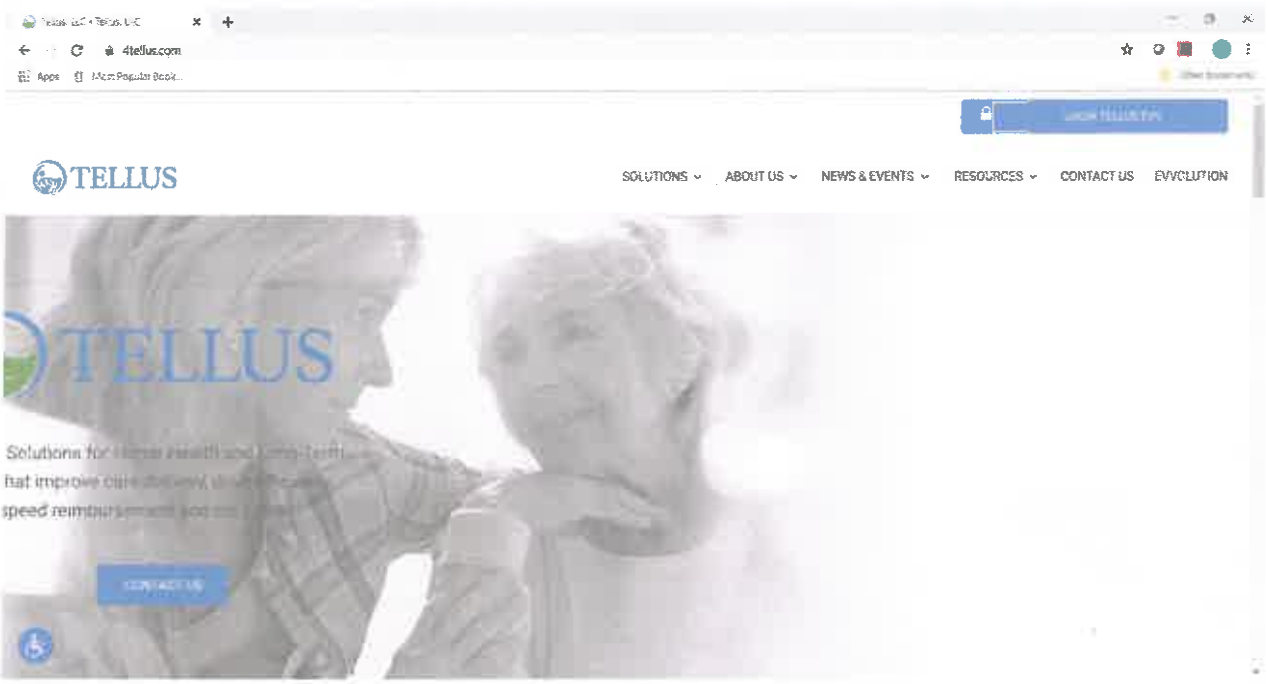
automatically whenever the terms of use are updated by Tellus.

SM073	4846	1	The solution should have the ability to establish user access to predefined Department levels including, but not limited to:
SM074	5016	2	Page level
SM075	5017	2	Field level
SM076	5018	2	Data element level

Yes, read/write data access can be controlled to any of the above levels by user role.

SM077	4847	1	The Vendor should provide a public facing website that provides access to a secure portal including, but not limited to:
SM078	4848	2	Instructions on how to use the secure site
SM079	4849	2	Site map
SM080	4850	2	Contact information

4tellus.com is a public website that offers a wealth of information about our products, service, and news and events about the EVV industry, register for training, or contact Tellus to schedule a demonstration. Users must have a login to access our secure application where they can use the administrator and claims functions, and access online user documentation



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.

After downloading the Mobile app, users will self-register before they receive a username and password to log into the Tellus EVV Mobile app. Self-registration requires that they enter a user name, password, their first and last name, email address, phone number, rendering provider ID/Medicaid ID if they have one, and Caregiver Type, When self-registration is complete, they will receive their user name and password via email from the Tellus System. This information will be required to log in to the Mobile App. Users will be asked to change their password the first time they log into the mobile app

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:
SM083	5021	2	Provider number
SM084	5022	2	Prior authorization number

SM085	5023	2	Medicaid ID number
SM086	5024	2	Date of service
SM087	5025	2	Claim number

Yes, the system makes use of challenge questions and required information for searches to control data access.

SM088	4755	1	The solution should allow a system administrator to reset user passwords.

Both the web-based consoles and mobile app have options where users can request a password reset. They will receive an email that requires a timed response in order to create a new password. Users can also contact their system administrator for a password reset.

SM089	4756	1	The solution should allow users to change their passwords on demand.

Both the web-based consoles and mobile app have options where users can request a password reset. They will receive an email that requires a timed response in order to create a new password. Users can also contact their system administrator for a password reset.

SM090	4852	1	The solution should have the ability to set and adjust password expiration dates.

Yes, the system user credentialing and management solution supports configuration of password expiration dates as well as password complexity, and number of allowed failed

password attempts.

SM091	5226	1	The solution should have the ability to warn the user that the Caps Lock is on when entering sign-on passwords.

The Tellus EVV Solution is browser-based. Browsers automatically provide this warning.

SM092	4231	1	The Vendor should establish an expiration schedule for system component required passwords to minimize system or user disruption.

Yes, the system user credentialing and management solution supports configuration of password expiration dates.

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)

Tellus ensures data security encryption of all information while in transmission and while at rest on electronic media storage devices. Required data is encrypted consistent with Federal Information Processing Standards (FIPS), and NIST cryptographic standards.

In RDS Databases:

- Encryption algorithm used is AES 256 Encryption
- Encryption algorithm used for one-way hashing is SHA256

SM094	4234	1	The solution should enforce password policies for length, character requirements, and updates for all users as agreed upon by the Department

Yes, the system user credentialing and management solution supports configuration of

password expiration dates as well as password complexity, user suspension policies, and number of allowed failed password attempts before user is locked out.

SM095	4241	1	The solution should allow self-service password resets.

Both the web-based consoles and mobile app have options where users can request a password reset. They will receive an email that requires a timed response in order to create a new password.

SM096	4243	1	The solution should send system-generated email notifications of password change events and expiration warnings at Department approved intervals.

Yes, password expirations are set as a number of days after the password is established or reset. The system provides communications to end users to prompt password reset.

SM097	4242	1	The Vendor should deactivate all system access for users immediately upon notification of termination, departure, or reassignment.

Yes, system access is terminated immediately.

SM098	4248	1	The solution should have the ability to lock out a user after a pre-determined number of unsuccessful login attempts.

Yes, the system user credentialing and management solution supports configuration of password expiration dates as well as password complexity, user suspension policies, and number of allowed failed password attempts before user is locked out.

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.

Tellus EVV will automatically suspend all users who have not accessed the solution within the period of time specified by DHHR.

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.

Yes, the system user credentialing and management solution supports configuration of password expiration dates as well as password complexity, user suspension policies, and number of allowed failed password attempts before user is locked out.

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.

Yes, both web portals and mobile app are configurable to terminate sessions after a period of user inactivity, typically 30 minutes.

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:
SM103	4750	2	Preventive Controls: Controls designed to prevent errors and unauthorized events from occurring
SM104	4751	2	Detective Controls: Controls designed to identify errors and unauthorized transactions that have occurred in the system.

SM105	4752	2	Corrective Controls: Controls designed to ensure that the problems identified by the detective controls are corrected.

Tellus takes data integrity very seriously to ensure compliance with the 21st Century Cures Act as well as payer and provider-specific policies and procedures. As such, Tellus requires third-party vendors to adhere to a minimum set of standards that represent best practices. Data from third-party EVV vendors is normalized as part of the import process. Regardless of the origination, the data is put into a common format and record layout, so it is consistent with the database layout and, ultimately, exposed to business rules as well as the portals or other application for visibility into care delivery.

Our solution is built on an open source platform with open standards and can interface with any system that adopts these standards, whether it employs ODBC, XML, flat file or other standards. Routine internal QA and validation is performed on reference data to insure conformity.

Tellus ensures that the design and implementation of applications takes into account risks as well as processing failures that may lead to a loss of integrity. Tellus takes steps to minimize risk by employing appropriate data integrity controls. Data integrity controls address:

The use of add, modify and delete functions to implement changes to data.

Procedures to prevent programs running in the wrong order or running after failure of prior processing.

The use of appropriate programs to recover from failures to ensure the correct processing of data.

- Protection against attacks using buffer overruns/overflows.
- A checklist for validation checking is prepared, activities documented, and the results kept secure. The checks to be incorporated include the following and can be manual:
- Session or batch controls, to reconcile data file balances after transaction updates.
- Balancing controls, to check opening balances against previous closing balances, namely: Run-to-run controls, file update totals, program-to-program controls, validation of system-generated input data.

- Checks on the integrity, authenticity or any other security feature of data or software downloaded, or uploaded, between central and remote computers.
- Hash totals of records and files.
- Checks to ensure that application programs are run at the correct time.
- Checks to ensure that programs are run in the correct order and terminate in case of failure, and that further processing is halted until the problem is resolved; and creating an automated log of the activities involved in the processing.

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.

The system currently contains similar warnings for download of PHI and can be enhanced with warnings as required by the Department.

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.

Yes, this type of reporting is defined via the Tellus Incident Response Policy.

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.

This mapping is complete and the documentation available upon request.

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.

Tellus acknowledges and agrees that Tellus staff will complete all security forms, such as acceptable use policy, user authorization form, and non-disclosure agreement and all other required documentation that is necessary before starting work under the contract. We will comply with all security requirements for our staff working at a secured DHHS site.

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.

The EVV platform is hosted on Amazon Web Services (AWS) Government Cloud and runs on 15 AWS data centers located in the continental US. AWS datacenters are distributed in geographic regions which include clusters of datacenters called Availability Zones. Every region is geographically isolated in terms of power and water supply, and each zone is similarly served by independent networks. Redundantly storing information in different datacenters in multiple regions, availability zones, and datacenters greatly reduces downtime, as the nearest available node is activated as a backup.

Each AWS datacenter is protected by four distinct layers of security:

- Perimeter Layer - Datacenters are physically enclosed by gates protected by security guards and intrusion detection technology
- Infrastructure Layer - Energy generators, fire suppression equipment, and ordinary and extraordinary maintenance systems protect the integrity of the data stored in the datacenter
- Data Layer - Access to server rooms is restricted, tightly regulated by authorization processes and constantly monitored
- Environmental Layer - The locations where AWS datacenters are built are screened for seismic activity and extreme weather, to minimize the risk of structural damage caused by natural occurrences

SM111	4263	1	The Vendor should provide the Department access to all facilities to conduct announced and unannounced visits of the Vendor's facilities.

Tellus hosts our solution on AWS Government Cloud. Amazon (AWS) does not allow customers to visit its data centers.

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.

Tellus hosts our solution on AWS Government Cloud. Amazon (AWS) does not allow customers to visit its data centers.

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.

Yes, the system includes utilities for the merger of recipient, caregiver, and provider data records.

SM114	4265	1	The solution should audit and track all activity specific to each user including, but not limited to:
SM115	4266	2	Invalid login attempts
SM116	4267	2	Transaction activities
SM117	4268	2	Track adds, changes, and deletes of individual member visit verification data
SM118	4269	2	Password changes
SM119	4270	2	Security question and/or Key creation
SM120	4271	2	Updates to security questions
SM121	4272	2	User navigation history

Yes, the above information is tracked by the solution user credentialing and management solution.

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)

Tellus policy requires annual security training per our HITRUST certification.

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:
SM124	4276	2	User Identification
SM125	4277	2	Machine/Internet Protocol Address Identification
SM126	4278	2	Time and Date of Action
SM127	4279	2	Actions Performed

The system includes an audit feature that is managed at the service layer. The system captures a snapshot before and after of each edited business object (recipient, provider, user, visit, claim, etc. records) along with the identity of the system or individual who made the change.

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.

Yes, the above information is tracked by the solution user credentialing and management solution.

SM129	4257	1	The Vendor should disable building and system access in real-time for staff upon termination, departure, or reassignment from the project.

Yes, per our Access Control policy.

SM130	4283	1	The solution should generate audit reports based on a request from authorized requestors at the Department.

Yes, audit reports will be made available upon request.

SM131	5288	1	The solution should have the ability to control access to member records based on user roles and system credentials.

Yes, the solution features a role-based architecture for the management of user access to functionality and data.

SM132	4247	1	The solution should support member-delegated authority including, but not limited to:
SM133	5161	2	Assistors
SM134	5162	2	Authorized representatives

Yes, the solution includes this type of delegated authority—notably for authorized representatives in the self-directed/participant-directed solution.

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.

One of the standard steps in our recruiting and vetting process is a qualification verification and background check. We verify the approved applicant's qualifications and conduct a management interview to determine applicants' skills and if the skills match a specific job appropriately. If an applicant is successful during the interview, a group of peers conducts a rigorous technical interview to assess knowledge, skills, and abilities. The group prepares questions in advance, seeks to confirm technical or functional skills, and confirms the manner in which the individual will respond to challenging situations. We consider both technical and behavioral responses when we assess the candidate's ability to fit into our project team.

If we proceed with an offer, we conduct an independent, third-party background investigation that includes confirmation of employment, salary, educational history, and reference/financial/credit and criminal records checks. We do not schedule any candidates to work on a client contract until we complete the background investigation. Our Corporate Security Office maintains a database of new hires subjected to a pre-employment background investigation. This database is checked as part of the prescreening process for our employees scheduled to perform on a customer contract. Additionally, our background check policy requires all employees to complete an annual background check successfully. A consumer reporting agency performs this check and reports felony level offenses. We will make sure the qualification verification and background check we perform for the project comply with your requirements. This policy reassures our customers that the staff members assigned to their projects pass both initial and ongoing background checks.

Tellus acknowledges and understands that all Tellus staff working on this project will be subject to a Criminal Background Check (CBC), and that Tellus will be solely responsible for the cost of the CBC. Tellus understands that the DHHR will review the CBC results and, at the DHHR's sole discretion, may request that Tellus staff members be replaced if their CBC results are unsatisfactory. Tellus does take exception to the process defined in RFP Exhibit K. Please see Attachment 3, Exceptions, of this proposal response for information regarding our exceptions. Tellus human capital resources will work with the DHHR to fulfill this requirement. Tellus

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.

Yes, as required per our HITRUST certification.

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.

Tellus undergoes annual penetration testing and external audits by an independent third party at our major data centers to review performance against identified control objectives and will provide the DHHR with reporting. We will work with the DHHR to remediate any identified vulnerabilities in a mutually agreed upon timeframe. Patching and corrections related to security vulnerabilities of a critical nature will occur within three (3) business days and those of a major nature within ten (10) business days.

Tellus' Security Operations Center (SOC) personnel monitor NIDS sensors 24/7 for security incidents. Tellus' SOC personnel provide Level 1 and 2 supports on security incidents and Security Engineering personnel provide Level 3 support for serious incidents. Tellus leverages Cisco as well as Open Source SNORT and McAfee in our IDS monitoring and reporting solution. For monitoring emerging information security threats and vulnerabilities, Tellus has established and formally documented Incident Response/Crisis Management (IR/CM) policies and procedures .The Incident and Crisis Response Center (ICRC) tracks, documents, and reports security incidents to higher level Tellus officials, and addresses accidental or unauthorized disclosure, modification, or destruction of ePHI or confidential information by technical or non-technical workers (support, janitorial, maintenance, and or vendors), operations staff (IT, managers, etc.), criminal acts, natural disasters, and/or labor strikes.

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.

Tellus will only allow DHHR approved users to enter an/or approve change request activities. This requirement will be documented in the Change Management Plan.

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)

Tellus EVV complies with the standards and protocols outlined in sections 1104 and 1561 of the Affordable Care Act.

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)

Tellus complies with the physical safeguard provisions of 45 CFR 164.310.

SM141	4754	1	The solution should allow local and central system security administrators to add and change permissions for local and central system access.

Tellus EVV is a SaaS-based application. Role-based permissions are set up by individual users at the entity level. DHHR EVV administrators will have the ability to add and change permissions for DHHR users.

Additional requirements related to adding and changing permissions can be defined and implemented during the solution planning and development phases of the project.

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.

Tellus will maintain agreed upon levels of security compliance during any interruption of normal operations. Contingency plans for the disruption of operations will be defined in the Disaster Recovery and Business Continuity Plan, one of the contract deliverables required by DHHR.

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.

Tellus will provide a comprehensive disaster recovery (DR) document as it relates to this project. The DR Plan is updated at least annually or any time a major system update or upgrade is performed. The Disaster Recovery Lead will be responsible for updating the entire document and permitted to request information and updates from other employees and departments within the organization to complete this task.

The DR Plan limits service interruptions to a period of 24 hours. However, because our systems are fully utilizing scalability, disaster recovery, high availability and monitoring features of AWS, we do not anticipate that recovery time will be anywhere close to 24 hours.

Our systems reside in Amazon Web Services. We utilize AWS disaster recovery, failover and elasticity capabilities. We do not maintain our own hardware or physical data centers instead running our system in 15 AWS data centers in VA, OH and CA. Utilizing various AWS regions and different physical data centers within same region ensures that the system is highly available and fault tolerant.

The server environment is virtualized. This allows for portability in case the disaster affects the datacenter when the application server is running. Within minutes, a new instance of the

same server will be launched in a different datacenter in a different AWS availability zone or region. As a result, downtime is cut to minutes instead of hours.

Using AWS, we achieve higher levels of fault tolerance for our applications by using Elastic Load Balancing to automatically route traffic across multiple instances and multiple Availability Zones (physical data centers). Elastic Load Balancing ensures that only healthy Amazon application server instances receive traffic by detecting unhealthy instances and rerouting traffic across the remaining healthy instances. If additional computing capacity is required, we have a system in place that will scale the application and database server layer to provide the level of service according to SLA.

The database is a critical component of the system. We use Amazon RDS (Relational Database Service) to host our database server. Amazon RDS runs on the same highly reliable infrastructure used by other Amazon Web Services. In production, we provision Multi-AZ DB Instances.

Amazon RDS synchronously replicates the data to a standby instance in a different Availability Zone (different datacenter). In case of failure of the primary node, Amazon RDS performs an automatic failover to the standby without the need for manual administrative intervention. When a failover is performed, there is a very short period during which the primary node is not accessible. We utilize many Amazon RDS features that enhance reliability for critical production databases, including automated backups, database snapshots, and automatic host replacement in case of primary database crash. In addition to synchronous replication, database backup snapshots are taken at regular intervals and sent to AWS S3 encrypted storage.

The comprehensive DR Plan will be provided to the Agency when it's modified, or at least annually, as a PDF file. At the Agency's request, in accordance to the best interests of the Agency, the DR Plan will be updated at no additional cost.

The DR Plan will be tested annually or after major infrastructure or system changes to ensure completeness and effectiveness of the existing Disaster Recovery Plan. Results of the DR Plan testing will be submitted to the Agency as soon as the test is complete - and at least annually.

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.

We will submit the technical documentation, including a final architectural diagram for each system environment, data dictionary, and high-level process flow diagram prior to contract signature. We will also negotiate the exact time frame for this delivery with DHHR prior to contract signature. WDH will review and approve any architectural changes, relative to interface points with DHHR and external data sources before we implement them. We will implement integration point architecture changes in the lower environments first, and then promote them to upper environments after completing formal system integration testing (SIT) and user acceptance testing (UAT) and receiving DHHR approval.

SM145	4307	1	The Vendor should ensure that all Vendor-owned hardware and software are configured securely, including but not limited to:
SM146	4308	2	Being protected by industry standard virus protection software, which is automatically updated according to a Department-approved schedule.
SM147	4309	2	Having all security patches installed that are relevant to the applicable operating system and all other system software and hardware.
SM148	4310	2	Maintaining compatibility with Department software and systems.
SM149	4311	2	Utilizing only licensed software and hardware solutions that have not been classified as End-of-Life (EOL).

Yes, per our Security, Acceptable Use, Physical Environmental Security, and Mobile Computing policies.

SM150	4312	1	The Vendor should ensure they are in compliance with the State and Department Information Technology Security and Privacy Policies.

Tellus is HITRUST certified and will meet any additional security and privacy policies per state policies.

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.

Yes, this type of activity is managed by the Tellus DevOps & Infrastructure team.

SM 152	4321	1	The Vendor should provide continuous monitoring of the solution using intrusion detection software (IDS).

Yes, Tellus operates intrusion detection/prevention software & hardware at all times and will make reporting available as required by the Department.

SM153	4322	1	The Vendor should provide reports at intervals as agreed upon by the Bureau from the intrusion detection software (IDS).

Yes, Tellus operates intrusion detection/prevention software & hardware at all times and will make reporting available as required by the Department.

SM154	4323	1	The Vendor should provide continuous monitoring of the solution using industry standard intrusion prevention software (IPS).

Yes, Tellus operates intrusion detection/prevention software & hardware at all times and will make reporting available as required by the Department.

SM155	4324	1	The Vendor should provide reports at intervals agreed upon by the Department from the intrusion prevention software (IPS).

Yes, Tellus operates intrusion detection/prevention software & hardware at all times and will make reporting available as required by the Department.

SM156	4328	1	The solution should have the ability to support non-disclosure of information.

Access to the EVV solution is tightly controlled using secure login ID and device access controls. System security is integrated into the system's basic design. We have a number of standard security features to make sure that only authorized users can access the system and its data, including user authentication through IDs and passwords, functional access controls, multiple firewalls and several different virus protection products. Data transmitted between external systems and our servers is protected by authentication and encryption, while secure file transfer protocols (SFTP) are always used for data file transmissions.

We do not use or disclose health information for any reason other than that mandated within the client requirements or otherwise required as a matter of law. We understand the significance of signing and adhering to the policies, protocols and procedures outlined by DHHR.

SM157	4429	1	The Vendor's Technical Call Center should have the ability to authenticate the caller/user as required by the Department.

Yes, Tellus will coordinate with the Department for technical/DevOps user authentication approach.

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.

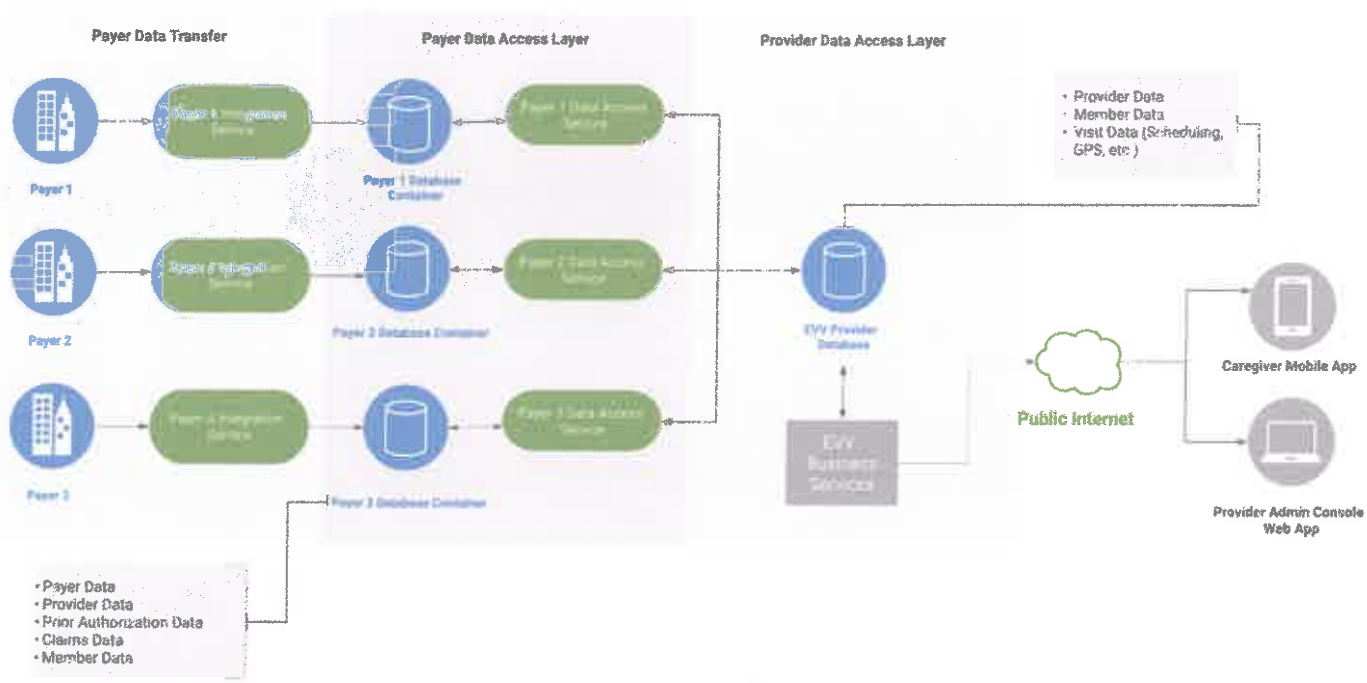
Tellus EVV is architected to support data collection and aggregation in sophisticated multi-payer environments. Each payer Tellus works with is set up in a physically segregated database. Data ingested from other vendors specifically associated with DHHR will be loaded into the DHHR database.

EVV data is stored in the Tellus EVV database. Views and reports are constructed to relate data from different databases into a logical view. This is accomplished behind the scenes employing a combination of code and business intelligence rules. We understand rules can

vary by payer, program, provider and even recipient. We use a business intelligence rules engine for the flexibility to support and change rules without custom software development.

This design provides data security and integrity for payers. It makes it easy for direct care workers to focus on member quality of care without worrying about different rules operating behind the scenes for various payers and provider agencies.

The diagram below depicts the multi-tenant architecture of the data collection component of our solution. The data aggregation component of our solution enables us to accept EVV data from all sources for State Medicaid reporting and oversight.



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.

Tellus EVV is 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. For example, typical messaging standards supported by the Tellus data interchange solution include:

- ANSI X.12 Electronic Data Interchange (EDI) including **834, 837, 835, 271, 272**
- HL7 (Health Level Seven) version 2 messages
- CDA (Clinical Data Architecture)/CDD (Continuity of Care Document)
- CSV (comma-separated variable)
- DICOM
- XML
- JSON
- NCPDP
- RAW
- JavaScript Batch
- Additional Data Types are support via API Libraries

Our flexible open architecture also allows custom and legacy interfaces to be easily added to support data sharing with systems that are not able to share information in one of the protocols that is native to the platform.

ATTACHMENT 9: IMPLEMENTATION SPECIFICATIONS APPROACH

Instructions: 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 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.

Responses should reference specifications and relevant mandatory requirements using the appropriate IDs from **Appendix I: Detailed Specifications and Attachment 6: Mandatory Requirements.** 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.

The Vendor is required to respond to the headings below to provide detail regarding its methodology for each project management component.

1 PROJECT MANAGEMENT METHODOLOGY

1.1 Policies & Procedures

Instructions: *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.*

Describe policies and procedures employed to ensure timely completion of tasks in a quality fashion.

Tellus assigns a PMP Certified Project Manager to each of our projects. The Project Manager maintains a project timeline, risk matrix and work breakdown structure for all key deliverables of the project.

We focus on rock solid delivery practices and the intentional creation of unparalleled client experiences. The project work plan will be developed by a PMP Certified Project Manager

who will manage this project. The Project Manager will communicate Project Status to DHHR on a weekly basis in an agreed upon format. The Project Manager will maintain a project timeline, a risk matrix, and a work breakdown structure for all key deliverables of the project.

The Level of Effort (LOE) for the project has been estimated from the analysis of the scope outlined in the RFQ. The activities have been grouped into development activities, implementation activities, training activities, deployment activities, customer service activities, and project oversight activities. These groupings provide the information required to provide a top-down estimate on the entire project based on the tasks needed to comply with the deadlines in the implementation plan. The top-down is one of the tools and techniques promoted by the PMI's best project management practices documented in the PMBOK©.

The project timeline will incorporate the required milestones and work required to successfully abide by the delivery dates outlined by DHHR in the RFP. The draft implementation plan, containing the initial draft schedule, will be provided within thirty (30) days of contract execution.

The phases required to complete the work will follow industry best practices for project management and software development. Project management phases may include project initiation, planning, executing, monitoring and controlling, and closing.

The software development staff utilizes the Agile / SCRUM methodology for developing projects. Using two-week sprints, the team provides constant feedback to the Project Manager and other key stakeholders for the project, ensuring that issues are identified early on and mitigated appropriately. In keeping with Agile best practices, a daily standup (meeting) is held to communicate progress and identify any impediments to progress.

The anticipated deliverables coinciding with project milestones needed to comply with the EVV System solicitation will include the deliverables listed below. Additional milestones may be required after the initial phase analysis of work with intermediate deliverables that are needed in the project plan to abide by the project dates.

PROJECT MILESTONES TIMELINE

#	MILESTONE	TIMELINE DAYS FROM CONTRACT EXECUTION
1	Project Initiation	31
2	Solution Planning 1	35
3	Solution Planning 2	44
4	Solution Design, Testing & Operational Readiness 1	77
5	Solution Design, Testing & Operational Readiness 2	107
6	Solution Design, Testing & Operational Readiness 3	141
7	Deployment 1	161
8	Deployment 2	177
9	Deployment 3	184

PROJECT DELIVERABLES TIMELINE

The following table represents the specific deliverables that must be completed to achieve each of the milestones highlighted in the table above:

TASK GROUP	TASK ID	WBS CONTROL NUMBER	PROJECT DELIVERABLES	TIMELINE IN DAYS
1	D001	1.1	Project Kickoff Meeting	6
1	D002	1.2	Change Management Plan	20
1	D003	1.3	Communication Management Plan	20
1	D004	1.4	Cost Management Plan	20
1	D005	1.5	Document Management Plan	20
1	D006	1.6	Modularity and Reusability Plan	24

1	D007	1.7	Project Work Plan	24
1	D008	1.8	Quality Management Plan	24
1	D009	1.9	Risk & Issue Management Plan	24
1	D010	1.10	Schedule Management Plan	30
1	D011	1.11	Scope Management Plan	30
1	D012	1.12	Staffing Management Plan	30
1	D013	1.13	Stakeholder Management Plan & Analysis	31
2	D014	2.1	Data Management Plan	27
2	D015	2.2	Data Security, Privacy & Confidentiality Plan	27
2	D016	2.3	Incident Management Plan	27
2	D017	2.4	Master Test Plan	34
2	D018	2.5	Privacy Impact Analysis	30
2	D019	2.6	Requirements Gap Analysis	30
2	D020	2.7	Requirements Management Plan	30
2	D021	2.8	Requirements Specification Document	44
2	D022	2.9	Requirements Traceability Matrix	28
2	D023	2.10	Safeguard Procedures Report	28
2	D024	2.11	Security Plan	28
2	D025	2.12	System Backup and Record Retention Plan	28
2	D026	2.13	System Requirement Document/User Stories	43
3	D027	3.1	Capacity Plan	38
3	D028	3.2	Configuration Management Plan	38
3	D029	3.3	Data Conversion Plan	45
3	D030	3.4	Data Conversion Test Cases	52
3	D031	3.5	Data Conversion Test Results	76
3	D032	3.6	Database Design Document & Data Models	38
3	D033	3.7	Detailed System Design Document	38

3	D034	3.8	Disaster Recovery & Business Continuity Plan	38
3	D035	3.9	Federal Certification & Review Management Plan	64
3	D036	3.10	Interface Inventory	94
3	D037	3.11	Load & Stress Test Cases	91
3	D038	3.12	Load & Stress Test Results	104
3	D039	3.13	Operational Readiness Plan	104
3	D040	3.14	Operational Readiness Test Scripts	104
3	D041	3.15	Operational Readiness Test Results	105
3	D042	3.16	Regression Test Cases	99
3	D043	3.17	Regression Test Results	119
3	D044	3.18	Reports & Forms Inventory	93
3	D045	3.19	System Integration Plan	99
3	D046	3.20	System Integration Test Cases	99
3	D047	3.21	System Integration Test Results	104
3	D048	3.22	Training Management Plan	122
3	D049	3.23	User Acceptance Test Cases	105
3	D050	3.24	UAT Results & Letter of Completion	140
4	D051	4.1	Cutover Play Book	142
4	D052	4.2	Federal Review Supporting Documentation	146
4	D053	4.3	Implementation Certification Letter	146
4	D054	4.4	Implementation Plan	104
4	D055	4.5	Operations Change Management Plan	160
4	D056	4.6	Operational Milestone Review	155
4	D057	4.7	Production Screenshots, Reports & Data to Certify	155
4	D058	4.8	Report Distribution Schedule	169
4	D059	4.9	Solution Health Monitoring Plan	162

4	D060	4.10	System Operations Plan	176
4	D061	4.11	System & User Documentation	183
4	D062	4.12	Training Materials	183
4	D063	4.13	Training Report	183
4	D064	4.14	Training Schedule	183
4	D065	4.15	Turnover & Closeout Management Plan	183
5	D066	5.1	Project Schedule	171
5	D067	5.2	Project Status Reporting	171
5	D068	5.3	Risk Register/Exception Plan	171
5	D069	5.4	Updated Project Management Components	171
5	D070	5.5	Updated Requirements Traceability Matrix	190
5	D071	5.6	Updated Training Management Plan	190

1.2 Work Plan

Instructions: 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:

Manage the work
Guide work execution
Document planning assumptions and decisions
Facilitate communication among stakeholders
Define key management review as to content, scope, and schedule

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.

The project management plan/initial work plan, as well as the procedures documentation and work breakdown structure, outlines an effective change control method for the review, revision, and approval of planning documents, testing processes, and other project deliverables. We recommend a change control board (CCB) be created to provide feedback on identified changes, to review and approve modifications. The CCB should be formed early in the project and shall include DHHR and Vendor stakeholders.

We will require the assistance of the State as it relates to the approval of the implementation plan. This would include timely and detailed feedback on the draft implementation plan.

Additional assistance required from the DHHR may be requested during the regular established meetings and/or communication methods to ensure timely response and/or approval of the stated assistance request. Our experience is that timely assistance is very beneficial during the initiating and planning phases of the project.

A communication plan shall be created to identify the best communication methods between the Vendor and the State and its identified stakeholders. The plan shall include proper expectations regarding the receipt and acknowledgement of information and requests and necessary dates, so as to engage both parties and outline the proper expectations. A mix of mediums shall be used, such as information repository, emails, and phone calls. Meetings to gather information, contractor statuses, issues, risks, and project statuses will be scheduled appropriately throughout the different phases of the project to ensure that communication is flowing between all project stakeholders. Meetings will have the overall goals of identifying risks, providing issue resolution alternatives, and capture project work effort and provide forecasting effort needed to stay on plan.

1.3 Issue Management

Instructions: 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.

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.

The Vendor should also detail any planned use of an automated solution to support issue management.

Tellus uses Atlassian Jira as our internal ticketing system during the implementation phase of our projects and maintains an open issues log as an Excel spreadsheet for joint review with our clients during project meetings. Tellus will manage open tickets for any issues on integrated Tellus software.

Tellus does not expect to use subcontractors for this implementation but as a matter of policy would manage any subcontractor issue logging and reporting unified with any Tellus issues.

Atlassian Jira is a SaaS-based automated support issue management system.

1.4 Risk Management

Instructions: The Vendor's proposal should describe the Vendor's risk management practices, the expected risk areas, and mitigation plans.

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.

Risks will be documented in a Risk Management Plan created as part of the overall project management plan. and as such will follow PMBOK© guidelines. The Risk Management Plan will be supplemented by a risk register that includes both impact and probability ratings, prioritizations, responses, and contingency plans to address each of the identified risks. The register will be managed by the Project Manager and will continue to change as the project progresses. Risk identification will be an activity that will continue through the completion of the contract.

Risk Management provides a proactive and collaborative means of augmenting project management on a project by addressing risk factors before they become project problems. The purpose of Risk Management is to ensure that risks associated with an IT project are well understood so they can be managed, planned for, and mitigated during the execution of the project. A risk is any factor that may potentially interfere with the successful completion of the project. Use of Risk Management illuminates and attacks the threats to a project as early as possible to allow for a successful outcome.

a. Risk Identification

Risk Identification typically occurs at the beginning of the project but may occur at any stage of the project and continues throughout the project's life cycle. Management must ensure that the project team openly and routinely discusses and analyzes risks throughout the life of the project. As risks are identified, a Risk Management Worksheet is filled out and completed. The worksheet is preferably automated in a Risk Management database. All information about each risk at the time of identification will be entered in the database. As each risk moves through the risk processes of Analysis, Planning, Tracking, and Control, new information will be added to the database. The Risk Management database is maintained with the current status of the risks and is used as the primary source for reporting and tracking.

Risk Identification is a recurring event; it is not performed once and then set aside. Risk identification begins at the time of Project Definition Plan (PDP) development and approval and continues throughout the life of the project. New risks may develop as the project matures and external and internal situations change.

b. Risk Analysis

Once risks have been identified, the next step is to analyze the risk item within the context of its consequence and its likelihood. Risk Analysis is a systematic method of identifying and evaluating the threats to a project, its vulnerabilities, and methods of minimizing or eliminating consequences due to threats. Assessing and analyzing a project's risks will help project managers make more informed decisions and ensure more successful outcomes. Risk assessment is not problem management but is a process that reduces the likelihood of problems occurring. Analyzing risks has three basic activities: evaluating attributes of risk,

classifying risk, and prioritizing risks. The objective of risk assessment is to transform risk data into decision-making information.

A. **Risk Exposure:** This is determined by evaluating two criteria: (1) The Probability of Occurrence and (2) The Consequence of Occurrence. The probability of occurrence is defined as the probability that the identified risk will occur and impact the program's success assuming no supplemental actions are taken at the time of assessment. The consequence of occurrence is defined as the magnitude of potential negative impact to the program/project if the risk should occur. The formula used for the Risk Exposure calculation is simple:(Probability of Occurrence) x (Consequence of Occurrence) = Risk Exposure. The Risk Exposure formula is used to create the following matrix scale:

B. **Time Frame:** Time Frame relates to how soon action is required to prevent a risk from occurring. Risks will be ranked so that the risks with the highest risk exposure and shortest time frame for action will be reviewed first. The dimension of time is a critical factor when evaluating Risk Exposure. Reaction time to a Risk Item can be a key element to the success of implementing the mitigation action. For the purposes of this Risk Management Plan, the time frames are specifically defined as how long until the Risk might become a problem: Immediate, Short (~ 1 month), Medium (~ 2 months), and Long (~ 4 months).

C. **Risk Severity:** Risks can then be sorted or prioritized so that the risks with the highest Risk Exposure are reviewed first. The risks with the highest Risk Exposure represent the top candidates for mitigation plans and regular tracking. Prioritizing risks in this manner enables the focusing of management attention, and project resources, effectively and efficiently.

c. Risk Planning

Risk planning is the function of deciding what, if anything, should be done with a risk. The objectives of risk planning are to ensure consequences and sources of the risk are known, assign responsibility, develop effective plans, and to produce over time, the correct set of actions that minimize risk and impacts (cost, schedule, quality) while maximizing opportunity and value. The risks with the highest Risk Exposure should be planned for mitigation first. Risk Action (Mitigation) Plans (RAPs) should be developed in phased 'levels. A Level 1 plan is first devised as the initial plan for sufficiently mitigating the risk. If the Level 1 plan is not achieving the desired result, then a Level 2 plan can be defined and

considered for implementation. Likewise, with a Level 3 plan, if necessary, in order to prevent the risk from becoming a major issue or problem on the project.

d. Risk Tracking

The objective of Risk Tracking is to collect accurate, timely and relevant risk information and to present it in a clear and easily understood manner appropriate to the group who receives the information. Tracking is a process in which risk data is acquired, compiled, and reported by the person(s) responsible for tracking, and mitigating risk. The risk reports generated during tracking are used by project personnel for/during Risk Control to make decisions about managing risks. Tracking updates the information associated with each risk to include measures, indicators, and triggers.

e. Risk Control

Risk Control is the process that takes the tracking status reports for the tracked and mitigated risks and decides what to do with them based on the reported data. The objective of Risk Control is to make informed, timely, and effective decisions regarding risks and their mitigation plans. The general process of controlling risks includes analyzing the status reports, deciding how to proceed, executing the decisions, and subsequently monitoring the risk and mitigation.

1.5 Quality Management

Instructions: 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.

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.

More specifically, the Vendor's approach to quality management should include, at a minimum, the following elements:

Management of the solution specifications. This includes the identification of inconsistencies between the specifications, project deliverables, and/or artifacts.

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.

Management of configuration management activities, including but not limited to the control and monitoring of the software library.

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.

The Vendor's approach to business process changes resulting of requests from DHHR.

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.

The Vendor's approach to the quality of work products developed and delivered by Vendor and the Vendor's subcontractors, if applicable.

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.

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.

The Vendor's organizational structure, and the roles and responsibilities of Vendor staff as they relate to quality management.

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.

Tellus believes the best way to describe our approach to Quality Management is to provide an example of one of our test plans. The detailed plan is included as Addendum C - Payer Integration Test Plan.

Tellus creates a test plan for each project based on the solution specifications. The following bullet points describe our process in more details:

- See attached sample Payer Integration Test Plan (Tellus Payer Integration Test Plan Sample 20190124.doc). Key points: Tellus maintains a versioned copy of the solution specifications with history on a SharePoint folder that is established for each project. The specifications are updated as necessary with red-line copies provider to our client throughout each project, with the final set up updates representing the "as-built" specifications. After production rollout then all specification updates are handled through our change order process.
- Tellus creates work tickets (Jira Stories and Subtasks) for each unit of development work in Atlassian Jira and creates the Requirements Traceability Matrix (RTM) by linking each Jira story back to the business requirement.
- Software Configuration Management (SCM) is managed through a build workflow that is based on Git (source code repository), Jenkins (software build orchestration), Flyway (database build orchestration), docker (containers) and Kubernetes (container orchestration). All system configuration is stored in a configuration server.
- See attached document POL-0EXE-08-ChangeControl for Tellus Change Control Policy.
- The test plan includes the mechanism for issue reporting, tracking, and resolution.

1.6 Change Management

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).

Tellus believes the best way to demonstrate our approach to Change Management is to share our internal document outlining our change management policy, See Addendum D - Change Management

In addition, the DHHR project management plan, as well as the procedures documentation, will outline an effective change control method for the review, revision, and approval of planning documents, testing processes, and other project deliverables. We recommend a change control board (CCB) be created to provide feedback on identified changes, to review and approve modifications. The CCB should be formed early in the project and shall include DHHR and Vendor stakeholders.

2 ORGANIZATIONAL CHANGE MANAGEMENT

Instructions: *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.*

The Vendor's proposed methodology should at a minimum address the following areas:

The Vendor's organizational change management methodology

Determination of the impact of change

Methods of responding to the change, process harmonization, and approach towards potential resistance

Methods for helping to promote successful change management

Lessons Learned regarding change management challenges

Tellus EVV is a COTS application configurable to meet your specific requirements thanks to our powerful business rules engine. Our methodology favors configuration over customization to accelerate implementation time, streamline testing and simplify change management.

The initial configuration is recorded in the CMDB (Configuration Management Database), provided through the Drools Business Rules Management System, which is an integral part of the solution. The configuration is therefore automatically logged and regularly maintained throughout the project lifecycle. Changes to the initial configuration are requested by the State and subsequently implemented and recorded in the integrated CMDB as they occur.

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:
PM002	5036	2	Rule deletion

PM003	5037	2	Rule modification
PM004	5038	2	Addition of new rules
PM005	5146	2	Business edits
PM006	5147	2	Others as defined by the Department

Tellus EVV is a SaaS-based application built from the ground up to provide maximum flexibility with minimal effort. Configuration settings, variable parameters and business rules that are separate from our code base provide the ability to deploy a highly flexible and adaptable solution for any environment very quickly. This includes rule deletion, rule modification, addition of new rules and business edits.

At the heart of the system's flexibility and adaptability is our Rules Engine. Tellus EVV makes use of the RedHat Drools Rules Engine. The solution is comprised of a core Business Rules Engine (BRE), a web authoring and rules management application (Drools Workbench) and an Eclipse IDE plugin for core development. Key features are as follows:

- Drools is a Declarative Rules Engine.
- The Drools Inference Engine uses Rete algorithm for pattern matching.
- Engine supports Forward (iterate) & Backward (goal seek) chaining.
- Business rules version control is managed with the rest of our source code using the Git source control system. Rules rollback uses the same mechanism as software rollbacks.
- The Drools engine provides full debugging capabilities, including support for code step-through with break points, and the ability to see which rules have fired. Eclipse IDE includes a plugin that visualizes the RETE tree.
- Drools Flow offers a workflow design functionality in the form of blocks. The user specifies exactly which rules are executed in which order under which conditions.

Business rules are generally defined by payer. However, they can be created at any level, using the following hierarchy:

- Jurisdiction (State)
- Payer
- Plan

- Program
- Provider
- Caregiver
- Recipient

This classification system enables DHHR to configure the EVV application at the program level. Program rules, services, policies and procedures and reimbursement rates can be defined at the program/provider level. Business rules can also be written based on these categories as well as at the field level. Because our business rules engine is a module independent of the software code base, rules can be changed during the term of the contract without the use of development resources, providing maximum flexibility.

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.

Access to components of the application and the ability to view and write to specific fields is controlled by secure, private login credentials as well as by role-based permissions. User roles are defined during the business requirements gathering phase of the project.

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)

Tellus software application architecture and processes support the Seven Standards and Conditions advocated by CMS as follows:

1. **Modularity Standard:** Tellus EVV is comprised of five major modules, or components, that operate together or individually. The modules work seamlessly together in a runtime

environment employing loosely coupled services. Real-time rendered service data is available for claims pre-adjudication and 837 submission to MMIS on the day services are completed. Payer adjudication data can be imported to EVV and made available to providers as soon as the payer transmits the information to Tellus. Tellus can accept standard 835 or proprietary data formats.

2. **MITA Condition:** Tellus will assist the State in documenting "As-Is" and "To-Be" environments of business, information and technical capabilities demonstrating an increasing MITA maturity level, complying with MITA 3.0. Tellus will also strive to identify and recommend opportunities to leverage the reuse of health care technologies within the State and among other states.
3. **Industry Standards Condition:** Tellus EVV is fully compliant with the following standards: a. Health Insurance Portability Act of 1996 (HIPAA) b. Health Information Technology for Economic and Clinical Health Act (HITECH) c. National Institute of Standards and Technology (NIST) Special Publication (SP) 800 d. Section 508 of the Rehabilitation Act, Americans with Disabilities Act (ADA) e. Federal Civil Rights Laws f. Section 1104 of the Affordable Care Act g. Section 1561 of the Affordable Care Act h. 45 CFR 164.316 and Administrative Rule 37.85.414
4. **Leverage Condition:** Tellus supports the open/hybrid EVV model and publishes standard open Application Program Interfaces (APIs) promoting interoperability across the Medicaid ecosystem by integrating with care management applications, third-party EVV vendors and MMIS.
5. **Business Rules Condition:** Tellus is passionate about understanding the perspectives of all EVV constituents. Our communications, outreach, training and customer support initiatives strive to promote a community of reliability, trust and respect. Our EVV solution supports accurate claims processing processes and procedures.
6. **Reporting Condition:** Tellus EVV collects and evaluates all the data necessary to evaluate the operation and performance of the EVV program to monitor and improve operations, transparency and accountability. AWS CloudWatch is used to monitor network traffic, bandwidth usage and bottlenecks that impede performance. Monitoring and auto-scaling systems provide the information required to diagnose system performance issues, errors and backlogs. Monitoring includes, but is not limited to, CPU, memory utilization, network and disk utilization. For the database server, we also monitor read/write latency, number of sessions and session performance. Our engineers get immediate notifications about all system issues. If these cannot be resolved immediately, notifications will be forwarded to the State and/or Providers as required based on service level agreements.

7. **Interoperability Condition:** Tellus uses Mirth Connect, an open source, cross-platform, bi-directional health care integration engine providing maximum flexibility to integrate with health information exchanges, public health agencies, human service programs and other community organizations as required.

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.

As a rule, our EVV application is updated on a quarterly basis with release notes shared with clients in advance to make them aware of enhancements and provide access to training materials if necessary. We will share these artifacts with the WDH no less than seven (7) business days prior to the release. If required due to changes in Federally mandated or National Standards compliance requirements (including, but not limited to, CMS, HIPAA, MITA) or technical issues, the applications may be updated off cycle. All changes will be monitored through the documented change control process and communicated to constituents in a timely manner.

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.

All changes will be monitored through the documented change control process and communicated to constituents in a timely manner, including sign off when required.

PM011	4199	1	The solution should have the ability to allow the modification of edits per the Change Management Plan.

Tellus EVV is a COTS application configurable to meet your specific requirements thanks to our powerful business rules engine. Our methodology favors configuration over customization to accelerate implementation time, streamline testing and simplify change management.

The initial configuration is recorded in the CMDB (Configuration Management Database), provided through the Drools Business Rules Management System, which is an integral part of the solution. The configuration is therefore automatically logged and regularly maintained throughout the project lifecycle. Changes to the initial configuration are requested by the State and subsequently implemented and recorded in the integrated CMDB as they occur.

Tellus EVV is a SaaS-based application built from the ground up to provide maximum flexibility with minimal effort. Configuration settings, variable parameters and business rules that are separate from our code base provide the ability to deploy a highly flexible and adaptable solution for any environment very quickly.

At the heart of the system's flexibility and adaptability is our Rules Engine. Tellus EVV makes use of the RedHat Drools Rules Engine. The solution is comprised of a core Business Rules Engine (BRE), a web authoring and rules management application (Drools Workbench) and an Eclipse IDE plugin for core development. Key features are as follows:

- Drools is a Declarative Rules Engine.
- The Drools Inference Engine uses Rete algorithm for pattern matching.
- Engine supports Forward (iterate) & Backward (goal seek) chaining.
- Business rules version control is managed with the rest of our source code using the Git source control system. Rules rollback uses the same mechanism as software rollbacks.
- The Drools engine provides full debugging capabilities, including support for code step-through with break points, and the ability to see which rules have fired. Eclipse IDE includes a plugin that visualizes the RETE tree.
- Drools Flow offers a workflow design functionality in the form of blocks. The user specifies exactly which rules are executed in which order under which conditions.

Business rules are generally defined by payer. However, they can be created at any level, using the following hierarchy:

- Jurisdiction (State)
- Payer
- Plan
- Program

- Provider
- Caregiver
- Recipient

This classification system enables DHHR to configure the EVV application at the program level. Program rules, services, policies and procedures and reimbursement rates can be defined at the program/provider level. Business rules can also be written based on these categories as well as at the field level. Because our business rules engine is a module independent of the software code base, rules can be changed during the term of the contract without the use of development resources, providing maximum flexibility.

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.

The Tellus EVV platform supports a manual visit verification process that is adaptable to program requirements throughout the contract period as directed by the Change Management Plan. The form of visit verification is captured on each visit record so if a visit is manually verified, it will be designated as "manual". Reporting and data analytics can help DHHR monitor and evaluate manually verified services.

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.

Tellus EVV boasts a robust reporting platform that supports pre-defined periodic reporting as well as ad hoc custom reporting. Standard reports and recipients of reports can be changed easily over the life of the contract as define in the approved Change Management Plan.

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.

Tellus provides complete documentation for our EVV system, which is updated across the life of the project, and includes Administrative System Documentation accompanied by both User Guides and PowerPoint training materials in writing, as well as both live and recorded webinar training sessions and video "snippets" for commonly asked questions. This material encompasses complete Administrative System Functionality and reporting capabilities.

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.

Standard training guides including system documentation, user guides, FAQs and training materials will be published online so that the most current documents are always available. User documents are published in both English and Spanish. We will verify accuracy of all translations. User documents are continually updated as features and functions are modified and introduced into the software. We will work with you in developing innovative approaches to deliver the training content that works for your constituents

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.

Tellus EVV is flexible and adaptable to the different business processes for each of the State's programs, including waivers and services. The solution will be configured for all programs requested during the business requirements phase, to include unique business rules for waiver programs if requested.

Business rules are generally defined by payer. However, they can be created at any level, using the following hierarchy:

- Jurisdiction (State)
- Payer
- Plan
- Program
- Provider
- Caregiver
- Recipient

This classification system enables the State of West Virginia to configure the EVV application at the program level. Program rules, services, policies and procedures and reimbursement rates can be defined at the program/provider level. Business rules can also be written based on these categories as well as at the field level. Because our business rules engine is a module independent of the software code base, rules can be changed during the term of the contract without the use of development resources, providing maximum flexibility.

User-based permissions, combined with flexible rules, allow the ability to customize user privileges by program. That means a provider can be granted the right to enter service tasks on one program by personnel type and not have that same access for another program.

Service task lists can vary and be customized based on program needs and rules. A configurable option is to allow direct caregivers to enter notes and/or alerts using their mobile device to effectively and efficiently communicate recipient status to provider administrators and/or case managers.

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.

System, portal and application updates will be released on an ongoing and as needed basis. Releases will maintain functionality, security and integrity of data. Releases that include new features and functionality may introduce additional configuration options for existing clients. Features and functions for upcoming releases will be communicated in advance of the release and existing clients will be educated about the options available as a result of the enhancements or modifications. They can adopt those changes by changing applicable business intelligence rules and configuration settings

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.

Any changes to the software processing workflow will be managed through the standard Tellus Change Management Process. See Addendum D, Change Management.

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.

The project management plan, as well as the procedures documentation, will outline an effective change control method for the review, revision, and approval of planning documents, testing processes, and other project deliverables. We recommend a change control board (CCB) be created to provide feedback on identified changes, to review and approve modifications. The CCB should be formed early in the project and shall include DHHR and Vendor stakeholders.

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.

See attached Addendum D, Change Management.

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.

Risks will be documented in a Risk Management Plan created as part of the overall project management plan. and as such will follow PMBOK© guidelines. The Risk Management Plan will be supplemented by a risk register that includes both impact and probability ratings, prioritizations, responses, and contingency plans to address each of the identified risks. The register will be managed by the Project

Manager and will continue to change as the project progresses. Risk identification will be an activity that will continue through the completion of the contract.

See Addendum E, Risk Management

PM022	4116	1	The Vendor should coordinate all testing activities as agreed upon by the Department.

After configuration or coding, the testing team verifies the deliverables of the implementation phase against requirements using our Requirements Traceability Matrix (RTM). The testing team follows the Software Testing Lifecycle (STLC) which is similar to the development cycle adopted by the development team.

All development activities, including testing, are driven by user requirements, system specs, the Interface Control Document and the Use Cases Document. These are the baseline documents that drive all coding and testing activities. Development and testing processes are closely interrelated, and development activities don't end when items are moved into testing. Errors and/or deficiencies are returned cyclically to the developers for correction and unit testing before attempting the testing process again. Customization of the system

isn't complete until all system testing is completed, approved and accepted by DHHR.

PM023	4117	1	The solution rules/procedures should allow and enforce multiple service limits for different service ranges including, but not limited to:
PM024	5198	2	Applicable test cases
PM025	5199	2	Expected test results
PM026	5200	2	Others as defined by the Department

The Test Plan describes the overall strategy for testing, the processes and the tools used for test execution, management, and reporting for each test level. The approach taken for each test level describes the test methods to verify the business, technical, and operational elements of the project. The testing process identifies the items to be tested, test objectives, test schedules, entry and exit criteria, reporting requirements, evaluation criteria, defect resolution, and environment requirements. We describe the development methods for the test conditions, scenarios and scripts. We also provide test criteria for non-testable requirements. See Addendum C - Payer Integration Test Plan

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.

Our planning for testing and test traceability begins early in the project, during the Requirements Analysis Phase. A System Test Plan will be submitted to DHHR for approval after completion of the Requirements Definition Phase (aka Requirements Analysis Phase). See Addendum C - Payer Integration Test Plan

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.

Users have access to a sandbox environment where they can practice and test features, functions and processes without impacting live data.

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.

See Addendum C - Payer Integration Test Plan In general the scope of testing for the department will be focused on a) any data transmitted to Tellus and b) any data received from Tellus.

PM030	4131	1	The Vendor should provide the Department weekly reports of testing status, including, but not limited to:
PM031	5201	2	Metrics on the number of tests completed
PM032	5202	2	Number of deferred or canceled tests
PM033	5203	2	Results of the tests executed
PM034	5204	2	Defects identified by severity level
PM035	5205	2	Corrective actions taken
PM036	5206	2	Others as defined by the Department

The quality team at Tellus is ultimately responsible for testing the EVV solution. This testing includes developing the test plan, setting up test cases, and performing different levels of required testing, such as system integration testing and performance testing. Once testing

is complete, we will provide the results to DHHR as requested. See Addendum C - Payer Integration Test Plan

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.

Our approach in the implementation process is to ensure that the system is functionally sound and operationally stable before the pilot or soft launch process. Our implementation team, quality assurance and test teams work together to thoroughly "shake out" the system.

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.

A Soft Launch/Pilot testing process is an excellent way to mitigate risk in the rollout process. In a Soft Launch, constituents work together to ensure the system is designed to perform as required end to end. A cross-section of selected users including payers, providers, administrators, and direct care providers who are trained and will go-live prior to statewide roll-out. The EVV solution is used for "live" visits which are collected at the point-of-care and processed through the system. The direct care providers who are participating in this pilot process may also do paper timesheets, so that those results can be compared to the automated results.

PM039	4144	1	The Vendor should provide written test results of the Pilot Testing to the Department within an agreed upon timeframe.

Once transactions begin to flow through the system during the Soft Launch, as described in the system flow diagram, all of the data is checked for accuracy and expected results. This process involves all participants, ensuring that the EVV system is receiving and accepting the visit data; and that all external interfaces (including the Data Aggregator and MMIS) are functioning in accordance to the specifications.

PM040	4145	1	The Vendor should provide the Department official written notification of readiness for full production operations after completion of Pilot Testing.

Anticipated versus actual results from the Soft Launch are documented and provided to the State to certify the system is ready for rollout to the remainder of the state.

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.

Interface Testing will be performed in conjunction with DHHR. Our Interface Test Plan will be a component of our QA Test Plan submitted to DHHR for approval. Our integration testing and implementation strategy is supported by our internally tested checklist documenting activities and check points required to be performed by both Tellus and our integration partner.

PM042	3987	1	The Vendor should conduct interface testing with external electronic visit verification (EVV) data partners approved by the Department.

Any external EVV data partners will need to be identified during the Design Management phase of the project. Management of interface testing with any external EVV data partners will be managed by the Tellus Integrations Team and will be both approved by the Department and regularly reported on by the Tellus project manager.

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.

All testing and training environments provided to DHHR are included in the project cost.

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.

The UAT environment reflects all functionality of the production environment, so it is a critical step for establishing system readiness before moving the system into production. We will provide training to a core group of State staff users as required by the RFP. State staff will receive end-to-end system training with detailed information about our system development and deployment methodology before user acceptance testing (UAT). This approach will help us perform a comprehensive UAT. A separate training environment (independent of our UAT environment) will be utilized for training.

PM045	4788	1	The Vendor should create, use, and make available to the Department, representative samples for testing edits, business rules, and workflow processing.

Yes, Tellus will make applicable samples available as part of the design process.

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)

Yes, Tellus will coordinate with the department to define requirements for scrubbed test data that does not contain PHI as an integral part of the test planning.

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.

Yes, See Addendum C - Payer Integration Test Plan. Tellus writes Test Cases in Jira Test Manager and is willing to share these with the Department.

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)

Tellus ensures that web portal design is in accordance with Departments and federal regulations and guidelines as requested.

PM049	5227	1	The solution should be developed and implemented in accordance with the project work plan.

A Project Manager will be assigned to the DHHR project on a full-time basis for the duration of configuration and implementation, until the EVV system is successfully implemented and accepted by the State. The Project Manager will have the authority to make day-to-day project decisions for Tellus and be responsible for all project management activities, including maintaining the project plan over the life of the project and validating that we satisfy all contract requirements. The Project Manager will schedule and host meetings with DHHR Subject Matter Experts (SMEs) to review business organization and functions along with the organization, functions, and data of existing information systems relevant to this project, and will host other important meetings, assign staff to those meetings as appropriate, and provide an agenda for each meeting. The Project Manager will lead weekly status meetings, including monthly milestone meetings and will record and distribute the minutes upon request. The minutes will include key decisions along with closed, active and pending issues. The Project Manager will also participate in all other State, provider

and stakeholder meetings as requested.

PM050	5244	1	The Vendor should conduct the following types of testing in support of the solution:
PM051	5245	2	Unit testing
PM052	5247	2	Iterative functional testing
PM053	5248	2	System integration testing (SIT)
PM054	5249	2	Interface testing
PM055	5250	2	Regression testing
PM056	5251	2	End-to-end testing
PM057	5252	2	Security testing
PM058	5253	2	Performance testing
PM059	5254	2	Usability/Accessibility testing
PM060	5255	2	Browser testing
PM061	5256	2	User acceptance testing (UAT)
PM062	5257	2	Data conversion testing
PM063	5258	2	Operational readiness testing (ORT)
PM064	5259	2	Other testing as identified by the Department and/or Vendor

The following components of the Development Phase ensure delivery of a system that successfully meets the defined standards and provides all functionality.

Unit Testing. Every requirement or system function has a use case that is documented and coded. Coding only takes place after use cases are documented. We base unit tests on the detailed requirements specified in the use case.

Iterative functional testing – To be performed using both manual and automated methods per the test plan.

System integration testing (SIT)/ Data conversion testing

– To be performed primarily using manual methods per the test plan.

Functional Demonstration. Upon completion of system test activities, Tellus performs a functional demonstration of the EVV so the State can ensure solution design requirements meet or exceed expectations.

Interface Testing. The main focus of interface testing is the proper and accurate transmission of files between external systems and the EVV system to ensure interfaces are operationally ready and stable.

System Acceptance Testing. System acceptance testing enables the State to test system functionality and ensure all system design requirements are met. Tellus develops a system acceptance plan that complies with all testing requirements and test participants follow detailed scripts developed by Tellus and approved by DHHR.

Regression Testing. Full regression testing is performed before the system acceptance test to avoid unacceptable test results. System coding is prepared in accordance with specific State of Michigan requirements defined in the requirements document to ensure that all parties agree on the project's scope and deliverables. Unit, integration and full regression testing is performed once coding is complete to ensure the system is functioning according to documented requirements.

End-to-end testing – To be performed using both manual and automated methods per the test plan.

Security testing – To be performed using both manual and automated methods per the test plan. Includes automated static- and dynamic-code testing.

Performance/Stress Testing. Performance breaks down into two components: volume and stress. The purpose of volume testing is to determine that sufficient capacity exists to handle anticipated peak volumes. These volumes are derived from the current program transaction history with an upward adjustment for anticipated trends in increased caseload or additional programs. The purpose of stress testing is to determine the maximum capacity of the system configuration as a whole and is, therefore, a more destructive type of test where transactions are run at an escalating rate until the system indicates that the maximum rate has been or is about to be reached. Tellus performs both volume and stress tests to identify the system's capacity and to rigorously test the software and hardware components.

Usability/Accessibility testing – To be performed as part of 508 compliance testing.

Browser testing - All supported browser and operating systems to be tested using primarily automated testing methods.

User acceptance testing (UAT) – To be performed primarily by the department with Tellus support per the test plan.

Operational readiness testing (ORT) – Final testing to be performed by Tellus and the Department prior to production rollout. Includes go-to-market readiness.

Network Performance Testing. A network performance test of the EVV system communication networks is conducted to ensure the network is capable of handling projected transaction volumes in the required response times and error thresholds.

PM065	5260	1	The Vendor should be prepared to assist the Department, as necessary, with User acceptance testing (UAT).

We will provide training to a core group of State staff users as required by the RFP. State

staff will receive end-to-end system training with detailed information about our system development and deployment methodology before user acceptance testing (UAT). This approach will help us perform a comprehensive UAT.

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.

Tellus will perform UAT to the extent possible without Department resources, but a portion of UAT includes testing of Department systems that will receive data from Tellus. This testing must be performed by the Department.

PM067	5262	1	The Vendor should complete regression testing subsequent to, but not limited to, the following:
PM068	5263	2	Deployment of new solution components
PM069	5264	2	Integration of each solution component into the primary solution
PM070	5265	2	Every migration of new build versions to each test environment
PM071	5266	2	Solution fixes
PM072	5267	2	Solution patches
PM073	5268	2	Solution releases
PM074	5269	2	Others as defined by the Department

Yes, Tellus will perform manual and automatic regression testing prior to every release.

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.

Yes, we expect regression testing to include SIT testing.

PM076	5271	1	The Vendor should obtain approval from the Department on which scenarios should be used for regression testing.

Yes, regression testing details will be addressed as part of the Test Plan.

PM077	5272	1	The Vendor should utilize end-to-end test cases in support of regression testing.

Yes, regression testing details will be addressed as part of the Test Plan.

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)

Yes, Tellus performs privacy and security testing that includes but is not limited to manual testing, automated testing, static code testing, and dynamic code testing prior to every release.

PM079	5274	1	The Vendor should propose testing scenarios and/or cases to the Department for their approval.

Test Plans will be submitted to DHHR for approval after completion of the Requirements Definition Phase (aka Requirements Analysis Phase).

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.

Our Performance/Stress Testing is broken down into two components: volume and stress. The purpose of volume testing is to determine that sufficient capacity exists to handle anticipated peak volumes. These volumes are derived from the current program transaction history with an upward adjustment for anticipated trends in increased caseload or additional programs. The purpose of stress testing is to determine the maximum capacity of the system configuration as a whole and is, therefore, a more destructive type of test where transactions are run at an escalating rate until the system indicates that the maximum rate has been or is about to be reached.

PM081	5277	1	The Vendor's performance testing should occur on a production ready version of the solution.

Tellus performs both volume and stress tests in NAME OF ENVIRONMENT to identify the system's capacity and to rigorously test the software and hardware components.

PM082	5278	1	The solution's performance testing environment should mirror the final production solution specifications.

Yes, Tellus UAT and Staging environments have the same topology as our production environment.

PM083	5279	1	The Vendor should perform usability/ accessibility testing for various types of users, including, but not limited to:
PM084	5280	2	Internal users
PM085	5281	2	External users
PM086	5283	2	Users with limited computer skills
PM087	5284	2	New user registration
PM088	5286	2	Users with disabilities

PM089	5287	2	Others as defined by the Department

Yes, usability and accessibility testing are carried out by third-party vendor as part of 508-compliance certification.

PM090	4133	1	The Vendor should conduct an Operational Readiness Review (ORR) prior to statewide implementation of the solution.

Yes, Tellus considers go-to-market/ Operational Readiness to be a parallel track on every implementation with the culmination in a set of Operational Readiness Review (ORR) sessions prior to production release.

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.

Tellus will work with DHHR to determine the anticipated volume for 30 calendar days of production-capacity and included a volume/stress test of that magnitude as part of our ORR to demonstrate the solution and Tellus staff is prepared for full production.

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).

Tellus will document and propose solutions and timeframes for corrective actions to all issues, problems and defects identified through the ORR.

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.

Tellus will prepare and submit to DHHR an ORR Report demonstrating Tellus and Tellus EVV are ready to begin operations.

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:
PM095	4969	2	Correct the report
PM096	4970	2	Verify the report
PM097	4971	2	Distribute or re-distribute the report
PM098	4972	2	Others actions as defined by the Department

Tellus will correct any report errors identified and correct the report with an agreed upon timeframe as defined in the Change Management Plan. At a minimum, actions will include correcting, verifying and distributing or re-distributing the report.

PM099	4089	1	The Vendor should assist the Department with specialized research and reporting as requested.

Tellus will assist DHHR with specialized research and reporting as defined.

PM100	4787	1	The Vendor should be able to test edits, business rules, and workflow processing and report on results.

Yes, business rule testing is an integral part of the test plan.

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.

See Addendum F - Vendor Transition or Termination Policy

PM102	4448	1	The Vendor should obtain Department approval of all scripts prior to implementation that will be used in the Technical Call Center.

Tellus will obtain DHHR approval of all Technical Call Center scripts prior to implementation.

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.

Yes, Tellus publishes a catalogue all any third-party solutions that are an integrated part of the Tellus solution.

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.

Information gathered during this phase of the engagement will be used to create the Functional Requirements Document, which will be presented to the State for review and approval.

Tellus will coordinate with the department to organize a series of Joint Application Development (JAD) sessions for this purpose.

The Functional Requirements Document will serve as the foundation for the Detailed System Design Document, which will describe how our EVV solution addresses the State's requirements.

PM105	522	1	The Vendor should maintain a requirements traceability matrix (RTM) throughout the lifecycle of the project.

After configuration or coding, the testing team verifies the deliverables of the implementation phase against requirements using our Requirements Traceability Matrix (RTM). The testing team follows the Software Testing Lifecycle (STLC) which is similar to the development cycle adopted by the development team.

PM106	5230	1	The Vendor should provide all stakeholders identified by the Department access to the requirements traceability matrix (RTM).

Yes, Tellus will make the RTM available to any interested stakeholders.

PM107	5231	1	The Vendor should document in the requirements traceability matrix (RTM) where each requirement is accounted for, including, but not limited to:
PM108	5232	2	Design documentation
PM109	5233	2	Code modules
PM110	5234	2	Test conditions
PM111	5235	2	Test scenarios
PM112	5236	2	Test cases
PM113	5237	2	Certification criteria
PM114	5238	2	Medicaid Information Technology Architecture (MITA) business areas and processes

PM115	5239	2	Medicaid Information Technology Architecture (MITA) Standards and Conditions
PM116	5240	2	Others as defined by the Department

Yes, Tellus will include this information in the RTM.

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.

Yes, Tellus will include this information in the RTM.

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.

Yes, Tellus prefers to incorporate JAD sessions into the requirements gathering and design phase.

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.

Our proposed solution is a configurable, scalable, extensible, COTS-based solution that is already designed and developed. Most of the RFP requirements will be met by the Optum solution for Delaware through configuration changes. Using the RTM developed from the RFP, we will determine if there are any functionality gaps in our solution that will require custom configuration. If any such gaps are identified, we will assign a team of technical resources to estimate the level of effort to configure the new functionality and present it to DHSS through the Change Control process. If DHSS identifies gaps that were not included

in the RFP scope of work, inclusion of those gaps will go through the formal change management process in which we will scope the configuration effort and cost associated with the change.

3 IMPLEMENTATION METHODOLOGY

Instructions: 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.

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:

Requirements Analysis and Solution Design Methodology

Solution Development

Data Conversion

Testing

Broadly speaking, Tellus Implementation Methodology includes: Initiation, Planning & Design, Execution & Build & Go-Live.

Implementation – Initiation and Planning & Design

Tellus completes the design objectives of the Implementation Plan by:

- Conducting discovery activities and requirements development, beginning immediately after the award of the Contract.
- Conducting familiarization activities to better understand the needs of the Medicaid Enterprise.
- Building the key planning documents for the Design Implementation Phase.
- Performing verification of deliverables.
- Designing the EVV system for, and receiving verification by, the State in joint meetings.

Implementation Plan – Execution & Build

Tellus completes the development objectives of the Implementation Phase by:

- Developing and constructing the system, based on approved requirements.

- Adapting the design and development in a timely manner to meet any approved changes in requirements that occur during the Implementation Phase.
- Performing unit, functional, integration, system and regression testing.

During the Execution & Build Phase, we use a time-tested, refined methodology for software development that includes thorough testing and detailed documentation to prepare and validate all systems for live operations. All system testing, as well as development of training materials, occurs during this phase. This process ensures that the EVV solution is configured and tested according to all applicable State and Federal regulations as defined and mutually agreed upon during the Planning & Design Phase, and as identified in the JAD session.

All development activities, including testing, are driven by user requirements, system specs, the Interface Control Document and the Use Cases Document. These are the baseline documents that drive all coding and testing activities. Development and testing processes are closely interrelated, and development activities don't end when items are moved into testing. Errors and/or deficiencies are returned cyclically to the developers for correction and unit testing before attempting the testing process again. Customization of the system isn't complete until all system testing is completed, approved and accepted by the State.

The following components of the Development Phase ensure delivery of a system that successfully meets the defined standards and provides all functionality.

- **Unit Testing.** Every requirement or system function has a use case that is documented and coded. Coding only takes place after use cases are documented. We base unit tests on the detailed requirements specified in the use case.

- **Functional Demonstration.** Upon completion of system test activities, Tellus performs a functional demonstration of the EVV so the State can ensure solution design requirements meet or exceed expectations.

- **Interface Testing.** The main focus of interface testing is the proper and accurate transmission of files between external systems and the EVV system to ensure interfaces are operationally ready and stable.

- **System Acceptance Testing.** System acceptance testing enables the State to test system functionality and ensure all system design requirements are met. Tellus develops a system acceptance plan that complies with all testing requirements and test participants follow detailed scripts developed by Tellus and approved by the State of Michigan.

- **Regression Testing.** Full regression testing is performed before the system acceptance test to avoid unacceptable test results. System coding is prepared in accordance with specific State of Michigan requirements defined in the requirements document to ensure that all parties agree on the project's scope and deliverables. Unit, integration and full regression testing is performed once coding is complete to ensure the system is functioning according to documented requirements.

- **Performance/Stress Testing.** Performance breaks down into two components: volume and stress. The purpose of volume testing is to determine that sufficient capacity exists to handle anticipated peak volumes. These volumes are derived from the current program transaction history with an upward adjustment for anticipated trends in increased caseload or additional programs. The purpose of stress testing is to determine the maximum capacity of the system configuration as a whole and is, therefore, a more destructive type of test where transactions are run at an escalating rate until the system indicates that the maximum rate has been or is about to be reached. Tellus performs both volume and stress tests to identify the system's capacity and to rigorously test the software and hardware components.

- **Network Performance Testing.** A network performance test of the EVV system communication networks is conducted to ensure the network is capable of handling projected transaction volumes in the required response times and error thresholds.

- **IVR Testing.** The IVR application is thoroughly tested to ensure the system properly accepts, processes and transfers calls while properly handling expected call volume.

- **EVV Documentation.** Tellus provides complete documentation for our EVV system, which is updated across the life of the project, and includes Administrative System Documentation accompanied by a Training Manual that encompasses complete Administrative System Functionality; and a Reports Manual describing all

standard and State-specific reports, as well as a description of the data files furnished to the State for internal report generation.

f. Implementation Plan Installation / Go-Live

Tellus completes the installation objectives of the Implementation Phase by:

Assisting the State of Michigan in creating User Acceptance Test (UAT) cases and in performing UAT of the system.

Providing a deployment plan leading to successful implementation of EVV.

Providing initial user training, staff preparation for operations, build-out of operations infrastructure and related supporting activities 30 days prior to the operation start date.

Our approach in the implementation process is to ensure that the system is functionally sound and operationally stable before the pilot or soft launch process. Our implementation team, quality assurance and test teams work together to thoroughly "shake out" the system.

A Soft Launch is always an excellent way to mitigate risk in the rollout process. In a Soft Launch, constituents work together to ensure the system is designed to perform as required end to end. A cross-section of selected users including payers, providers, administrators, recipients and direct care providers are trained and will go-live prior to statewide rollout. The EVV solution is used for "live" visits which are collected at the point-of-care and processed through the system. The direct care providers who are participating in this pilot process may also do paper timesheets, so that those results can be compared to the automated results.

Once these transactions begin to flow through the system, as described in the system flow diagram, all of the data is checked for accuracy and expected results. This process involves all participants, ensuring that the EVV system is receiving and accepting the visit data; and that all external interfaces (including the Data Aggregator and MMIS) are functioning in accordance to the specifications. Anticipated versus actual results are documented and provided to the State to certify the system is ready for rollout to the remainder of the state.

Another benefit of the Soft Launch is that adjustments can be made in the training programs if something seems difficult or not intuitive to the pilot team. Adjustments to the

web-based console and the reporting system can also be made once the results are analyzed. Reporting "dashboards" can also be enhanced during this phase to monitor any specific issues encountered during the pilot. The live data flowing through the various integration programs is also a good test of the bi-directional communication processes.

At this point, the State has received all feedback, and we are ready for a Statewide launch. With the lessons learned by all parties, the remaining users should experience a smooth and positive start to their EVV program.

During all phases of the implementation, all necessary artifacts required for mandatory go-live readiness are collected and stored. Additional assistance required from the State may be requested during the regular, established meetings and/or communication methods to ensure timely response and/or approval of the stated assistance request. Our experience is that timely assistance is very beneficial during the initiating and planning phases of the project.

3.1 Requirements Analysis and Solution Design Methodology

Instructions: 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.

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 Vendorto create usage scenarios and detailed business process workflows.

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.

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.

The solution design and its multiple components should be developed in conjunction with the Project Work Plan as follows:

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.

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.

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.

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.

The Vendor's proposed approach to requirements analysis and solution design should also include detail on the following:

Process for identifying and resolving gaps between the Vendor's and DHHR's understanding of an RFP specification.

How the solution's design will include collaborative design with functional and technical subject matter experts.

*How the Vendor intends to obtain DHHR approval on **RFP** specifications.*

Description of how the proposed solution will fulfill the Medicaid Information Technology Architecture (MITA) requirements.

Design documentation for all those project deliverables delivered during the Solution Planning and Solution Design, Testing, and Operational Readiness taskgroups.

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.

Solution Design is arguable the most important part of the engagement. Making sure requirements are properly captured, understood and agreed upon is the first step to building and deploying a successful program. Tellus completes the design objectives of the Implementation Plan by:

- Conducting discovery activities and requirements development, beginning immediately after the award of the Contract
- Conducting familiarization activities to better understand the needs of the Medicaid Enterprise
- Building the key planning documents for the Design Implementation Phase
- Performing verification of deliverables
- Designing the EVV system for, and receiving verification by, DHHR in joint meetings

To confirm our understanding of requirements provided by DHHR, Tellus will develop and submit for review the following deliverables during the Solution Planning Phase of the Engagement:

- Requirements Management Plan
- Requirements Specification Document
- Requirements Traceability Matrix
- System Requirement Document/User Stories
- Detailed System Design Document
- Configuration Management Plan
- Database Design Document & Data Models
- Capacity Plan
- Modularity and Reusability Plan
- Data Management Plan
- Data Security, Privacy & Confidentiality Plan

This body of documents prepared, reviewed and agreed upon will serve as the foundation for the development of the solution. These are living documents that will be updated through the course of the development of the solution, through testing and up to user acceptance certification as requested through the Change Management Process.

3.2 Solution Development Methodology

Instructions: 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.

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.

The Vendor's proposal should present a narrative description of the Vendor's proposed approach to solution development, including the Vendor's proposed:

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:

Regular system maintenance, performance optimization, resource capacity utilization, capacity planning, and capacity expansion.

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.

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.

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.

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.

Methodology and approach to ensure that the developed solution meets design criteria.

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.

Tellus completes the development objectives of the engagement by:

- Developing and constructing the system, based on approved requirements
- Adapting the design and development in a timely manner to meet any approved changes in requirements that occur
- Performing unit, functional, integration, system, regression testing and user acceptance testing

During the Execution & Build Phase, we use a time-tested, refined methodology for software development that includes thorough testing and detailed documentation to prepare and validate all systems for live operations. All system testing, as well as development of training materials, occurs during this phase. This process ensures that the EVV solution is configured and tested according to all applicable State and Federal regulations as defined and mutually agreed upon during the Planning & Design Phase, and as identified in the JAD session.

All development activities, including testing, are driven by user requirements, system specs, the Interface Control Document and the Use Cases Document. These are the baseline documents that drive all coding and testing activities. Development and testing processes are closely interrelated, and development activities don't end when items are moved into testing. Errors and/or deficiencies are returned cyclically to the developers for correction and unit testing before attempting the testing process again. Customization of the system isn't complete until all system testing is completed, approved and accepted by DHHR.

3.3 Data Conversion Strategy, Approach, and Timeline

Instructions: 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).***

The Vendor's proposal should also describe how the Vendor will ensure data integrity and consistency through all phases of the project.

Data Integration is a core competency for Tellus, we understand the current Operating

Environment requires sharing data across platform solutions and that data integrity is the key to successfully managing Medicaid programs. Tellus is currently integrated with MMIS, Agency Management and other third-party vendor systems as depicted in the graphic below.

Successfully developing and managing a series of bi-directional integrations will begin at the Project Initiation Phase by developing a Data Conversion Plan and a System Integration Plan. As the Solution is defined, the plans will evolve into an Interface Inventory and supporting Test Cases. Interface testing focuses on the proper and accurate transmission of files between external systems and the EVV system to ensure interfaces are operationally ready and stable.

Tellus will test each Interface and submit Data Conversion and System Integration Test Results prior to the Deployment of the EVV platform.

3.4 Testing

Instructions: 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.

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.

The DHHR defines the types of testing as follows:

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.

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.

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.

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.

Interface Testing: Interface testing ensures the completeness of interface development and the readiness of developed interfaces for integration in the wider system.

Regression Testing: Regression testing assesses the integrity of the solution subsequent to the deployment of new solution components and/or fixes.

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.

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.

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.

Usability/Accessibility Testing: Usability testing ensures the solution user interface design takes into account usability considerations for its target user groups.

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.

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.

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.

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.

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.

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:

All aforementioned testing types, as well as any others the Vendor plans to deploy

Timing for execution of each testing type

Usage of tools the Vendor proposes be used in support of each testing type

Testing environments to be used in support of each testing type, and for all necessary testing activities

Validating the traceability of requirements throughout the full testing process

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.

The Vendor's proposal should also present a narrative description that includes the following:

Approach to completion of the Solution Design, Testing, and Operational Readiness task group's testing-related deliverables.

Approach to obtaining DHHR's approval of the testing-related project milestones including the proposed acceptance criteria for each milestone.

Approach to:

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

Developing test cases and scripts to thoroughly test system functionality

Supplying documentation of each testing type

Preparing data for each testing type

Details on the support the Vendor intends to supply during UAT, such as the Vendor's approach to:

Developing the UAT Plan, scripts, cases, timeline, and supporting processes

Preparing test data

UAT results analysis, identification of defect severity, and defect resolution

Defect tracking, repair, and reporting

UAT final report that includes:

A written certification letter certifying that UAT was successfully completed

A list of all defects and issues

A list of all resolved critical defects and/or issues

The Vendor's proposal should also include detail on the approach to ORT including details on:

ORT approach

ORT final report that includes:

A written certification letter certifying that UAT was successfully completed

A list of all defects and issues

A list of all resolved critical defects and/or issues

Tellus provides complete documentation for our EVV system, which is updated across the life of the project, and includes Administrative System Documentation accompanied by a Training Manual that encompasses complete Administrative System Functionality; and a Reports Manual describing all standard and State-specific reports, as well as a description of the data files furnished to the State for internal report generation.

This documentation is initiated during the solution planning phase and is the foundation for unit tests conducted throughout the system design phase as well as the development of user acceptance test cases conducted at defined milestones and at the end of the development phase.

The following components of the Development Phase ensure delivery of a system that successfully meets the defined standards and provides all functionality.

- **Unit Testing.** Every requirement or system function has a use case that is documented and coded. Coding only takes place after use cases are documented. We base unit tests on the detailed requirements specified in the use case.
- **Functional Demonstration.** Upon completion of system test activities, Tellus performs a functional demonstration of the EVV so the State can ensure solution design requirements meet or exceed expectations.
- **Interface Testing.** The main focus of interface testing is the proper and accurate transmission of files between external systems and the EVV system to ensure interfaces are operationally ready and stable.
- **System Acceptance Testing.** System acceptance testing enables the State to test system functionality and ensure all system design requirements are met. Tellus develops a system acceptance plan that complies with all testing requirements and test participants follow detailed scripts developed by Tellus and approved by the State of Michigan.
- **Regression Testing.** Full regression testing is performed before the system acceptance test to avoid unacceptable test results. System coding is prepared in accordance with specific State of Michigan requirements defined in the requirements document to

ensure that all parties agree on the project's scope and deliverables. Unit, integration and full regression testing is performed once coding is complete to ensure the system is functioning according to documented requirements.

- **Performance Load/Stress Testing.** Performance breaks down into two components: volume and stress. The purpose of volume testing is to determine that sufficient capacity exists to handle anticipated peak volumes. These volumes are derived from the current program transaction history with an upward adjustment for anticipated trends in increased caseload or additional programs. The purpose of stress testing is to determine the maximum capacity of the system configuration as a whole and is, therefore, a more destructive type of test where transactions are run at an escalating rate until the system indicates that the maximum rate has been or is about to be reached. Tellus performs both volume and stress tests to identify the system's capacity and to rigorously test the software and hardware components.
- **Network Performance Testing.** A network performance test of the EVV system communication networks is conducted to ensure the network is capable of handling projected transaction volumes in the required response times and error thresholds.

Once User Acceptance Testing is complete, the UAT results and Letter of Completion will be delivered to DHHR and Operational Readiness Test Scripts and their Results will move the project to the Deployment Phase.

4 Deployment Methodology

Instructions: 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:

Implementation/Rollout Planning

Implementation Methodology and Timeline

Issues, Challenges, and Risks

Lessons Learned

See our response to each component in the appropriate section below:

4.1 Implementation/Rollout Planning

Instructions: The Vendor's proposal should describe the Vendor's methodology, tools, and techniques for implementation/rollout planning. The Vendor should include what specific staging, readiness, and deployment techniques it will use to determine the proper sequencing of deployment processes and functions required for successful implementation.

The Vendor's proposal should include, but not be limited to, details on its approach and methodology for the following:

Completing all Solution Deployment task group-related deliverables

Obtaining approval of all Solution Deployment task group-related deliverables and milestones

Completing operational readiness and operational readiness testing (ORT)

Documenting emergency back-out strategy

Completing Pilot testing

Confirming stakeholder readiness for new solution implementation

The Vendor's proposal should also include details on its approach to supporting and/or supplying:

System documentation

User documentation

Reports

Report distribution schedule

Production environment, including the final production schedule

Data conversion

Pre-implementation training

Updates to project management plans for operations

Tellus begins Deployment Rollout Planning during the Project Initiation phase of the engagement. Each of the deliverables associated with Solution Deployment is incorporated into our project team along with a deliverable date and the Tellus resource responsible for delivering that artifact.

Each phase prior to the deployment of the solution must be completed with the end goal in mind, deploying an EVV solution that meets the goals and objectives of DHHR. To accomplish that the following activities supported by the appropriate documentation must be planned, refined and executed throughout the engagement:

- Stakeholders are prepared to begin using EVV to verify visits and submit claims
  - Operations Change Management Plan
  - Operational Milestone Review
  - Report Distribution Schedule
  - System & User Documentation
  - Training Materials
  - Training Report
  - Training Schedule
  - Training Sessions
- EVV solution is transitioned to production, supporting deliverables include
  - Cutover Play Book
  - Federal Review Supporting Documentation
  - Production Screenshots, Reports & Data to Certify
  - Implementation Certification Letter
  - Implementation Plan
  - Solution Health Monitoring Plan
  - System Operations Plan
  - Turnover & Closeout Management Plan

Prior to Production Rollout, initial user training, staff preparation for operations, build-out of operations infrastructure and related supporting activities must be completed.

Our approach in the implementation process is to ensure that the system is functionally sound and operationally stable before the pilot or soft launch process. Our implementation team, quality assurance and test teams work together to thoroughly "shake out" the system.

A Soft Launch is always an excellent way to mitigate risk in the rollout process. In a Soft Launch, constituents work together to ensure the system is designed to perform as required end to end. A cross-section of selected users including payers, providers, administrators, recipients and direct care providers are trained and will go-live prior to statewide rollout. The EVV solution is used for "live" visits which are collected at the point-of-care and processed through the system. The direct care providers who are participating in this pilot process may also do paper timesheets, so that those results can be compared to the

automated results.

Once these transactions begin to flow through the system, as described in the system flow diagram, all of the data is checked for accuracy and expected results. This process involves all participants, ensuring that the EVV system is receiving and accepting the visit data; and that all external interfaces (including the Data Aggregator and MMIS) are functioning in accordance to the specifications. Anticipated versus actual results are documented and provided to the State to certify the system is ready for rollout to the remainder of the state.

Another benefit of the Soft Launch is that adjustments can be made in the training programs if something seems difficult or not intuitive to the pilot team. Adjustments to the web-based console and the reporting system can also be made once the results are analyzed. Reporting "dashboards" can also be enhanced during this phase to monitor any specific issues encountered during the pilot. The live data flowing through the various integration programs is also a good test of the bi-directional communication processes.

At this point, DHHR will have received all feedback, and we are ready for a Statewide launch. With the lessons learned by all parties, the remaining users should experience a smooth and positive start to their EVV program.

During all phases of the implementation, all necessary artifacts required for mandatory go-live readiness are collected and stored. Additional assistance required from the State may be requested during the regular, established meetings and/or communication methods to ensure timely response and/or approval of the stated assistance request.

4.2 Implementation Methodology and Timeline

Instructions: The Vendor's proposal should describe an effective implementation and deployment strategy to meet DHHR's specifications and help ensure State compliance with mandatory EVV deadlines defined in the Cures Act.

The Vendor's Initial Work Plan and work breakdown structure (WBS) in ***Attachment 5: Initial Work Plan*** *should include a sufficient level of detail to show the tasks and phasing strategy to deliver full solution functionality and the proposed implementation timing for both PCS and HHCS.*

Please refer to Attachment 5 and related Addendums to review the draft of our Initial Work Plan and WBS.

4.3 Issues, Challenges, and Risks

Instructions: DHHR is interested in any information that may help identify issues, clarify the specifications, reduce risk of the procurement, and identify issues and challenges of designing and implementing the proposed solution.

The Vendor's proposal should highlight any concerns or recommendations in this section.

Tellus is confident in our ability to develop a successful EVV platform with DHHR. Change always presents challenges but with committed partnerships challenges, issues and risks are recognized, discussed and overcome.

4.4 Lessons Learned

Instructions: DHHR would find it helpful to understand what the Vendor sees as the successes and primary challenges in the implementation of similar systems. In order to gain this insight, DHHR would like to draw upon the Vendor's experiences with similar projects.

The Vendor's proposal should describe any "lessons learned" from the Vendor's relevant experience and how those lessons learned will impact the Vendor's approach to this project.

The modular architecture for Tellus EVV and the rules hierarchy were developed based on business requirements gathered to construct a versatile EVV platform for our clients. The rules and configurations continue to be updated, as required, based on lessons learned, provider feedback and refinement of claims adjudication processes and details.

Having fully deployed our solution for multiple payers, we bring to future deployments the benefit of lessons learned along the way. Key lessons learned during previous engagements throughout program design, development, deployment and operations and maintenance phases include the following:

- Quality of member care trumps all other considerations when establishing business rules, policies, and procedures.

- Provider adoption requires consistent, frequent outreach and training.
- Providers are extremely knowledgeable about program details and valuable sources of information.
- Access to appropriate program and technical client resources is a significant key to success.
- A soft launch with a subset of providers and a limited retention of current claims processing capability is important to test business rules, configuration and integrations without penalizing providers.
- Curious, helpful, motivated Customer Support resources are a huge asset to program integrity and technical innovation.

Innovative techniques and functionality we developed and implemented as a result of these learnings include:

- Refinement of the mobile app user interface to incorporate bigger fonts and buttons, consistent colors throughout the app and reduced number of steps to complete the required workflow.
- Multi-payer support because many direct attendants work for more than one provider, and many providers are members of more than one payer network.
- Customized Consumer-Directed Services (CDS) module to support the unique requirements of that community.
- Modern, modular tools to better support the following EVV program functionality:
  - Aggregation o Integration
  - Dashboard Visualization & Customization o Reporting
  - Business Intelligence Rules

5 TRAINING

Instructions: *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:*

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.*

Approach to development, maintenance, and implementation of the Training Management Plan, including methodologies addressing:

Assessment of internal and external training needs, including gap analysis

Approach to user training, supporting all business processes as identified in the RFP

Delivery of end-user training throughout the solution's implementation

Development and use of online tutorials, online help, online policy and procedure manuals, and hard copy user manuals for the delivery of training

Development and use of live, web seminar, and video-based training

*The target audiences for training, including **DHHR** staff, Vendor staff, clients, providers, and third-party stakeholders that work in the system*

Plan to provide and/or leverage existing DHHR training facilities to perform end-user training detailed in this section

Tools that the Vendor will use to support training

The planned curriculum for each system user role and audience

Initial training schedule

Version control and maintenance of training documentation

Training evaluation, including the use of evaluation survey tools to determine whether the trainings produced the expected results

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

Approach to "train-the-trainer" activities during the Operations phase

Approach to role-based training during both implementation, and maintenance and operations

Approach to development of training materials

Approach to training evaluations

At Tellus, our EVV implementation is supported by a thorough and accessible training program designed to meet the needs of individual users including those with disabilities. Accommodations adhere to all State and Federal laws, rules, regulations and guidelines. Training sessions and related materials are available in English and Spanish. Training

incorporates all the following elements at the appropriate level for the User role that the training session is designed for:

- System access and log-on
- Data entry and updates
- Visit capture and validation
- Visit maintenance/updates to EVV visit transactions
- Clock-in/Clock-out methods
- Access and creation of reporting
- Customer Service (system troubleshooting, issue reporting, complaints, etc.)

Tellus will track completion of training for all users and report data in the EVV Vendor Monthly Performance report and at the request of the State of Michigan. User training is role-based, with sessions and materials geared to these roles:

- Direct care providers receive hands-on, step-by-step instruction on use of the mobile app and alternative verification methods. They also act as trainers, and we provide training on how to instruct and immediately support recipients during the sign-off phase.
- Consumer-Directed Services Employers are trained to use the Consumer-Directed Console and related timesheet functionality.
- Fiscal Management Services DHHR staff are trained to use the FMS portal as well as trained how to provide instruction and immediate support for Consumer-Directed Employers and their direct care providers.
- Provider DHHR Administrators receive in-depth training on the Administrator Console, the Claims Console and the Mobile App so they can assist employees and peers on use of the system and troubleshoot minor issues on site.
- Individuals in Billing and Financial roles receive training related to use of the Claims Console and the reporting features available within it.
- State Staff receive high level end-to-end system training as well as hands-on, step-by-step instruction for use of the State level Tellus EVV Console.
- Managed Care Organizations users receive hands-on, step-by-step instruction for use of the MCO level Tellus EVV Console.
- Recipients are engaged through focus groups initially to gain understanding of outreach and training needs. Our outreach campaigns are designed to raise awareness and promote the benefits of the EVV system. Online training is provided to recipients, particularly for consumer-directed members, to support them in navigating the system.

Direct care providers act as supporting trainers in explaining the sign-off phase of the process to recipients.

Training is delivered in a multi-modal approach that includes:

- Live, face-to-face training. During the initial implementation, a series of regional face-to-face, hands-on training events are scheduled in the months and weeks leading up to the State of Michigan's Go Live date. These training events include a variety of sessions covering topics designed to address the needs of State users, DHHR administrators and direct care providers, including special training for recipients and their designated representatives who are enrolled in a consumer-directed program.
- Live, interactive, role-based webinars. Trainers walk attendees through step-by-step instruction, based on their role as noted above. Attendees are encouraged to submit specific training or demo requests in advance of the session so live training can be tailored to the audience's needs. A question and answer session is held during the last 10 minutes of each session. If time doesn't allow for all questions to be asked and answered during the session, attendees can submit questions via email for individual response and follow-up.
- Online training and support center. Our easy-to-use, easy-to-access web-based training and support center offers a centralized location for access to training resources including user guides, FAQs, recorded training sessions, video tutorials and easy access to request additional support from our help desk.
- Sandbox Environment. Users have access to a sandbox environment where they can practice and test features, functions and processes without impacting live data.
- Train the Trainer. We encourage the State and provider agencies to identify certain individuals to receive in-depth training and serve as the resident experts at their site. These individuals play an important role in helping onboard new users and act as a liaison between Tellus training staff and their site to ensure their needs are always met in a timely fashion.
- Ongoing Refresher Courses and New Feature Training. Training sessions are available on an ongoing basis for new users and anyone needing a refresher. Tellus training staff also provides outreach and training to coincide with the release of new features and functionality.
- Printable Reference Materials. Reference materials included on the online training and support center are easily printable or downloadable.

- Simple User Guides and Tip Sheets. These guides will be shared with direct care providers and recipients to support their ongoing effective use of the system.
- Ongoing Communications. We also provide regular, ongoing communications with users to communicate tips and tricks, upcoming release information, important dates and other pertinent information. This includes offline means of communication, such as targeted mail campaigns as well as an active social media effort.

Tellus provides complete documentation for our EVV system, which is updated across the life of the project, and includes Administrative System Documentation accompanied by a Training Manual that encompasses complete Administrative System Functionality; and a Reports Manual describing all standard and State-specific reports, as well as a description of the data files furnished to the State for internal report generation.

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:
TN002	5176	2	Members or Legal Representative
TN003	5177	2	Direct Care Workers
TN004	5178	2	Provider Agencies
TN005	5197	2	The Department
TN006	5179	2	Other as defined by the Department

In our experience, Outreach should begin early in the planning process and continue post-deployment during the operational phase of the project. We communicate with all relevant audiences specified by DHHR. To lay the proper groundwork to facilitate ongoing communications, Tellus recommends the following:

1. Maintain a list of participating providers including contact information particularly phone numbers and email addresses.

2. Outreach to the community with multiple email blasts for provider, member and direct care provider alerts as well as care managers.

3. Email all affected EVV users anytime any functional changes to the system occur, which should include the changes made and the release notes.

4. For global communications and training sessions, Tellus recommends the State of Michigan have a beta group review communication materials and training information to provide feedback and advice prior to release.

TN007	3974	1	The Vendor should provide training at the time of registration.

Tellus will develop a training plan and schedule to support users throughout the implementation process in a variety of modalities. Training at the time of registration can be accommodated.

TN008	4146	1	The Vendor should collaborate with the Department and the stakeholder community to develop strategies to train members receiving services.

Tellus will collaborate with DHHR and the stakeholder community to develop strategies to train members receiving services. This training is likely to vary among programs and service delivery models.

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.

During the initial implementation, a series of regional face-to-face, hands-on training events are scheduled in the months and weeks leading up to the DHHR Go Live date. These training events include a variety of sessions covering topics designed to address the needs of State users, DHHR administrators and direct care providers, including special training for recipients and their designated representatives who are enrolled in a consumer-directed program.

We encourage the State and provider agencies to identify certain individuals to receive in-depth training and serve as the resident experts at their site. These individuals play an important role in helping onboard new users and act as a liaison between Tellus training staff and their site to ensure their needs are always met in a timely fashion.

TN010	4152	1	The Vendor should provide written training materials for both in-person and web-based training options.

Our easy-to-use, easy-to-access web-based training and support center offers a centralized location for access to training resources including user guides, FAQs, recorded training sessions, video tutorials and easy access to request additional support from our help desk.

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.

Tellus will submit training materials to DHHR for review and approval at least 5 days prior to the date of the first training session.

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)

Our EVV implementation is supported by a thorough and accessible training program designed to meet the needs of individual users including those with disabilities. Accommodations adhere to all State and Federal laws, rules, regulations and guidelines.

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 sessions and related materials are available in English and Spanish.

TN014	4156	1	The Vendor should obtain independent verification of the accuracy of all translations made pursuant to language and accessibility requirements.

User documents are published in both English and Spanish. We will verify accuracy of all translations.

TN015	4158	1	The Vendor should provide web-based training available to users throughout the life of the solution.

Our easy-to-use, easy-to-access web-based training and support center offers a centralized location for access to training resources including user guides, FAQs, recorded training sessions, video tutorials and easy access to request additional support from our help desk.

TN016	4160	1	The Vendor should provide a detailed approach to user training with respect to solution modifications.

Training sessions are available on an ongoing basis for new users and anyone needing a refresher. Tellus training staff also provides outreach and training to coincide with the release of new features and functionality

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.

Tellus will track completion of training for all users and report data in the EVV Vendor Monthly Performance report and at the request of DHHR.

TN018	4162	1	The Vendor's training records should be included in the data available for reporting.

Tellus will compile training records and include them in the data available for reporting based on DHHR specifications.

TN019	4168	1	The Vendor should provide a user manual to all users.

Our user manuals are located in our online training and support center and are easily printable or downloadable.

TN020	4169	1	The user manual should be subject to Department approval.

The user guides are currently universal for all users of the Tellus EVV System. Any training materials (PowerPoint decks or other materials) that are unique to the West Virginia program will be subject to Department approval.

TN021	4170	1	The user manual should be available online and in hard copy upon request of the user.

Reference materials included on the online training and support center are easily printable or downloadable.

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)

User manuals are designed to meet the needs of individual users including those with disabilities. Accommodations adhere to all State and Federal laws, rules, regulations and guidelines.

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)

The user manual can be translated into any language specified by DHHR.

TN024	5289	1	The solution should support workforce security awareness through such methods including, but not limited to:
TN025	5290	2	Security reminders (at login or screen access)

TN026	5291	2	Training reminders
TN027	5292	2	Online training capabilities
TN028	5293	2	Training tracking
TN029	5294	2	Others as defined by the Department.

Tellus supports workforce security awareness including:

- Security reminders
- Training reminders
- Online training instructions
- Training tracking
- Custom requirements outlined by DHHR can be accommodated.

6 CMS CERTIFICATION

Instructions: 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.

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.

Tellus software application architecture and processes support the Seven Standards and Conditions advocated by CMS as follows:

1. **Modularity Standard:** Tellus EVV is comprised of five major modules, or components, that operate together or individually. The modules work seamlessly together in a runtime environment employing loosely coupled services. Real-time rendered service data is available for claims pre-adjudication and 837 submission to MMIS on the day services are completed. Payer adjudication data can be imported to EVV and made available to providers as soon as the payer transmits the information to Tellus. Tellus can accept standard 835 or proprietary data formats.

2. **MITA Condition:** Tellus will assist the State in documenting "As-Is" and "To-Be" environments of business, information and technical capabilities demonstrating an increasing MITA maturity level, complying with MITA 3.0. Tellus will also strive to identify and recommend opportunities to leverage the reuse of health care technologies within the State and among other states.

3. **Industry Standards Condition:** Tellus EVV is fully compliant with the following standards: a. Health Insurance Portability Act of 1996 (HIPAA) b. Health Information Technology for Economic and Clinical Health Act (HITECH) c. National Institute of Standards and Technology (NIST) Special Publication (SP) 800 d. Section 508 of the Rehabilitation Act, Americans with Disabilities Act (ADA) e. Federal Civil Rights Laws f. Section 1104 of the Affordable Care Act g. Section 1561 of the Affordable Care Act h. 45 CFR 164.316 and Administrative Rule 37.85.414

4. **Leverage Condition:** Tellus supports the open/hybrid EVV model and publishes standard open Application Program Interfaces (APIs) promoting interoperability across the Medicaid ecosystem by integrating with care management applications, third-party EVV vendors and MMIS.

5. **Business Rules Condition:** Tellus is passionate about understanding the perspectives of all EVV constituents. Our communications, outreach, training and customer support initiatives strive to promote a community of reliability, trust and respect. Our EVV solution supports accurate claims processing processes and procedures.

6. **Reporting Condition:** Tellus EVV collects and evaluates all the data necessary to evaluate the operation and performance of the EVV program to monitor and improve operations, transparency and accountability. AWS CloudWatch is used to monitor network traffic, bandwidth usage and bottlenecks that impede performance. Monitoring and auto-scaling systems provide the information required to diagnose system performance issues, errors and backlogs. Monitoring includes, but is not limited to, CPU, memory utilization, network and disk utilization. For the database server, we also monitor read/write latency, number of sessions and session performance. Our engineers get immediate notifications about all system issues. If these cannot be resolved immediately, notifications will be forwarded to the State and/or Providers as required based on service level agreements.

7. **Interoperability Condition:** Tellus uses Mirth Connect, an open source, cross-platform, bi-directional health care integration engine providing maximum flexibility to integrate with health information exchanges, public health agencies, human service programs and other community organizations as required.

To make sure we achieve certification objectives, we follow the CMS Medicaid Enterprise Certification Life Cycle (MECL) release and updated checklists, which include greater alignment to MITA, the Seven Conditions and Standards, and recent federal legislation. In 2017, CMS updated the MECL and Required Artifacts to include an Operational Milestone

Review (R2) before the operations go-live of the system, in addition to the traditional Certification Final Review (R3) at the end of the system stabilization period.

While final guidance around certification of EVV Systems by CMS has yet to be issued, Tellus agrees that in the future, the EVV System will need CMS certification. We will work cooperatively with the State to achieve this certification. CMS has not yet issued guidelines for EVV System certification; if CMS has still not issued certification guidelines and all other Phase 4 deliverables have been accepted, Tellus will invoice for those completed items and will invoice for the certification deliverable when certification has been achieved.

We align our efforts to ensure the delivered solution conforms to MITA 3.0 standards and with all of the required checklists items for modular certification, such as:

- Business Area Checklist
- General Checklists:
- Information Architecture Checklist
- Access and Delivery Checklist
- Integration and Utility Checklist
- Intermediary and Interface Checklist
- Standards and Conditions Checklist

Additionally, our technical and advisory teams are ready to support every phase of the certification process with the creation of the required documentation in the MECT V2.2, like:

- Project Management Plan
- Schedule/Milestones & Burn-down Charts
- Risk Register/Exception Plan
- Test Plan
- Working MMIS module(s) and software
- Earned Value/Velocity Management Report
- Database Design and DED
- Data Conversion/Management Plan
- Contingency/Recovery Plan
- Test Reports/Validated Product Reports
- System Design Document (SDD)
- System Requirement Document
- Product Documentation (User and Training Manuals)
- HIPAA Statemen

Tellus routinely monitors CMS communications and will remain in alignment with all future updates.

CMS recently published Medicaid Enterprise Certification Toolkit Version 2.3 (MECT v2.3) that applies to all MMIS and related state technology solutions excluding EVV. EVV requires a streamlined, outcomes-based approach to achieve certification. This approach focuses on demonstrating alignment with specific business outcomes. EVV certification is structured around the following elements:

- Pre Go-Live Operational Readiness Review
- Post Go-Live Certification Review (six months or more after Go-Live)
- Outcome statements
- Evaluation criteria and required evidence corresponding to outcome statements to evaluate the system's functionality and compliance with laws, regulations, and industry good practices
- Key performance indicators (KPIs) reported quarterly to support the outcome statements and track performance of the system over time

Tellus welcomes the opportunity to support DHHR in the new CMS outcomes-based certification process.

ATTACHMENT 10: MAINTENANCE AND OPERATIONS SPECIFICATIONS APPROACH

Instructions: Maintenance and Operations specifications ensure that the solution is fully functional and performing optimally until the end of the lifecycle. 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. 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).

OPERATIONS

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:
OP002	4716	2	The estimated and actual hours allocated to each change request
OP003	4717	2	Specific personnel assigned to each change request
OP004	4718	2	Scheduled completion date for each change request
OP005	4719	2	Total cost if the maximum allowed hours are exceeded on any approved change request
OP006	4720	2	Any change to current operational costs
OP007	4721	2	A separate total for equipment requirements (if applicable) related to the modification
OP008	5008	2	Others as defined by the Department

Tellus will track and provide DHHR access to process metrics and other detail as defined in the approved Change Management Plan. Information included in the plan will include:

- Estimated and actual hours allocated to each change request
- Specific personnel assigned to each change request

- Scheduled completion date for each change request
- Total cost if the maximum hours are exceeded on any approved change request
- Changes to current operational costs
- Equipment costs are not applicable
- Other information as requested by DHHR

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.

Tellus will review new patches of the software products as part of the routine maintenance process, and we will work with the DHHR on the application of patches for software and firmware within the solution. We first apply the patches to the non-production environment. After testing and sign-off, we apply them to the production environment.

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.

The Change Management Plan will include a policy related to software system updates will be defined and communicated to the project team. As a rule, our EVV application is updated on a quarterly basis with release notes shared with clients in advance so they are aware of enhancements, and we provide access to training materials if necessary.

If required due to changes in Federally mandated or National Standards compliance requirements (including but not limited to CMS, HIPAA, MITA) or technical issues, the application may be updated off cycle. All changes will be monitored through the documented change control process and communicated to constituents in a timely manner.

Tellus will inform the DHHR in advance of any scheduled maintenance. The following information will be communicated in advance for approval:

- Specific system functionality impacted by the maintenance, or modification/enhancement changed
- Planned implementation date
- Downtime, system unavailability, start and end time
- Communication plan to notify users and stakeholders
- A contingency plan in the event of implementation issues

Alerts will be pushed to the web-based consoles and via email in advance of any downtime so users are made aware and can plan accordingly. Scheduled maintenance will occur during off hours to ensure the least amount of impact.

OP011	4745	1	The Vendor should provide the Department with detailed documentation that provides all fixes and functionality for each release.

As a rule, our EVV application is updated on a quarterly basis with release notes shared with clients in advance so they are aware of enhancements, and we provide access to training materials if necessary.

System, portal and application updates will be released on an ongoing and as needed basis. Releases will maintain functionality, security and integrity of data. Releases that include new features and functionality may introduce additional configuration options for existing clients. Features and functions for upcoming releases will be communicated in advance of the release and existing clients will be educated about the options available as a result of the enhancements or modifications. They can adopt those changes by changing applicable business intelligence rules and configuration settings

OP012	4747	1	The Vendor should maintain version control and provide the Department with current system and user documentation.

Tellus provides ongoing training anytime a new release includes functionality or system changes that impact users. We also update training materials to coincide with the release and will make sure materials are updated prior to functionality or system changes. Materials will be accessible in electronic format for all users. All training materials will be provided to DHHR for review prior to initiating training sessions.

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.

Tellus will review new security patches of the software products as part of the routine maintenance process, and we will work with the DHHR on the application of security patches for software and firmware within the solution. We first apply the patches to the non-production environment. After testing and sign-off, we apply them to the production environment.

OP014	3960	1	The solution should provide the ability for the provider agency to review billing prior to submitting for payment.

Completed visits display on a Work List that is accessible from the web portal. There are three statuses for completed visits:

- New: New are newly completed visits that have not been through the Tellus pre-adjudication process which happens automatically based on rules set by your organization. These visits usually are completed daily. New visits/claims cannot be released until they have been through the Tellus pre-adjudication process, and when the process has been completed, the status of each visit will change to either Matched or Unmatched.
- Matched: Matched visits are ready to be released for payment. All information from the visit matches the prior authorization, service codes, recipient address and date and time of visit.
- Unmatched: Unmatched visits have errors or are missing information. A User with the appropriate role authorization can click a visit to view details of the visit and to see the errors and edits needed.

Users with the appropriate role-based authority can review all visits (including Matched) before they are submitted for payment.

OP015	5130	1	The solution should provide the ability for the provider agency to review and correct billing errors prior to submission.

All completed visits display on a Work List that is accessible from the web portal. Claims with the status Unmatched have errors or are missing information. Users with the appropriate role-based authority can drill down within any visit to see visit detail and to correct information as needed.

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:
OP017	5131	2	No authorization
OP018	5132	2	Expired authorization
OP019	5133	2	Reasons that prevented claims from filing
OP020	5134	2	Edits made to claims
OP021	5135	2	Others as defined by the Department

Reporting is available as defined, via both standard and ad hoc reporting capabilities. Visits completed without a valid authorization (missing or expired) and those missing elements required for matching are available (these missing elements would be a subset of the list of reasons that prevented claims from filing. Reports on edits made to visits can be made available as outlined in the requirements specifications document. Basically, any action and/or edits can be tracked and reported on by the Tellus system.

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:
OP023	5100	2	Browser-based

OP024	5101	2	Portable Document Format (PDF)
OP025	5102	2	Excel
OP026	5103	2	Comma-Separated Value (CSV)
OP027	5172	2	Others as defined by the Department

Contact Center reporting can be provided upon requested schedule and/or as needed, often as part of monthly standard reporting processes. Contacts may include calls, emails, web requests and/or chat.

OP028	4522	1	The solution should track metrics for each type of correspondence generated in the solution.

Inbound contacts may include calls, emails, web requests and/or chat, and volumes can be broken out by channel. All calls are recorded. Tracking is in place for emails, web requests and chat, and counts or other information is available upon request.

OP029	4526	1	The solution should track the status of notices that are moving through the generation process.

Contacts and their progress and resolution are tracked within a ZohoDesk ticketing system, and current status is always available (Open, Active, Resolved).

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.

Contact resolution timeframes are tracked, and delivery timeframes can be created and reminders can be sent and/or displayed as requested.

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.

Correspondence (client communication) is tracked when issued, reminders sent, or reissued/updated as requested.

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)

Tellus can provide annual statement on SOC audit as requested.

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.

Tellus can provide annual statement and action plan for remediation as requested.

OP034	4253	1	The solution should archive and store user profiles for a period of time agreed upon by the Department.

User profiles are archived and available upon request.

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.

Tellus has operationalized incident reporting and the associated policies and procedures. These documents are available for review and approval upon request.

OP036	4164	1	The Vendor should detail the performance metrics and targets used to monitor the effectiveness of technical support by phone.

Tellus gathers, reviews and monitors and can report on performance metrics and targets used to monitor the effectiveness of technical support by phone. Sample metrics include totally call volume (during and after business hours) Average Speed of Answer, Abandon Rate, Number of Calls that choose to leave a voice mail and other metrics as determined would be useful.

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.

Tellus utilizes a ZohoDesk ticketing system that is configured to provide an immediate response acknowledging the receipt of all email inquiries and that will include a ticket number for future reference, in addition to establishing a timeframe for the response.

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.

The Tellus Technical Support/Production Operations Team is available to troubleshoot email inquiries as requested, although for production-impacting issues email is not recommended. A status of production-impacting issues can be provided within 1 hour of request, and resolution is targeted within 4 hours of request. Should an issue need further escalation, customer will be provided ETA.

OP039	4167	1	The Vendor should document inquiries and provide the Department with routine reports regarding reasons for technical support requests.

Inquiries and other technical support requests and the resulting resolutions are tracked, and the following information is recorded in Zoho Service Desk:

- Initial complaint/inquiry
- Caller identification
- Date & time
- Message
- Steps taken to remediate
- Final resolution

Routine reports are available that classify inquiries as to the type received.

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.

Tellus is familiar with the importance of documenting procedural actions and improvements that occurred as a result of a complaint to the helpdesk. This information is available for submission to the Department on an agreed upon schedule.

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:
OP042	4928	2	Hours of operation
OP043	4929	2	Options for leaving messages after hours
OP044	4930	2	Options for leaving messages based on queue hold times and designated intervals as defined by the Department
OP045	4931	2	Recording of informational messages as defined by the Department

The help desk is accessed by a U.S.-based, toll-free telephone number that is operational 24/7/365. The number is connected to our help desk supported by English and Spanish speaking staff (and other languages upon request).

The interactive voice response system informs callers of the help desk hours of operation and provides them the option of leaving a message, both during and after normal business hours. Options for leaving messages are configurable based on queue hold times and/or designated intervals as defined by the Department.

Recording of informational messages as defined by the Department is also available upon request.

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:
OP047	5108	2	Average speed of answer
OP048	5109	2	Interface processing time
OP049	5110	2	Request time for report generation
OP050	5111	2	Others as defined by the Department

The Tellus Solution has the ability to record and report on the performance and utilization of resources within the overall system, including ASA, interface processing time, request time for ad hoc and standard report generation and others defined by the Department.

OP051	4500	1	The Vendor should document and maintain technical specifications associated with the solution including, but not limited to:
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.
OP053	4502	2	Complete specifications for all software, environments, and hardware used to support the solution.
OP054	4939	2	Others as defined by the Department

We will submit the technical documentation, including a final architectural diagram for each system environment, data dictionary, and high-level process flow diagram prior to contract signature. We will also negotiate the exact time frame for this delivery with DHHR prior to contract signature. DHHR will review and approve any architectural changes, relative to interface points with DHHR and external data sources before we implement them. We will implement integration point architecture changes in the lower environments first, and then promote them to upper environments after completing formal system integration testing (SIT) and user acceptance testing (UAT) and receiving DHHR approval.

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:
OP056	4940	2	Hardware
OP057	4941	2	Environment
OP058	4942	2	Network specifications
OP059	5106	2	Others as defined by the Department

Because our solution is cloud hosted and accessed using personal computers, smart devices and operating systems, there are no limitations to the number of concurrent users who can access the application. The application is highly scalable with additional capacity managed by adding virtual machines as required to make sure performance standards are not compromised.

OP060	4661	1	The solution should provide real-time solution performance data.

Tellus monitors all components of the EVV platform real time using automated tools. Our infrastructure team is alerted immediately if any performance metrics are reporting abnormal results.

OP061	4663	1	The solution should report on total processing times based on user-defined queries.

Tellus monitors processing times using automated tools that monitor application performance.

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.

Tellus EVV retains audit logs including exception reports and error logs. Tellus can make these available to DHHR in a standard format for review upon request.

OP063	4740	1	The solution should allow the Department's administrator to view, filter, sort, and search the error log(s).

Tellus EVV retains audit logs including exception reports and error logs. Tellus can make these available to DHHR in a standard that will provide the DHHR administrator with the ability to view, filter, sort and search the logs.

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.

Tellus will notify DHHR if any releases of third-party software are known to create problems with the current version of our software.

OP065	4773	1	The solution should schedule and support file transfers as requested and agreed upon by the Department.

Data interchange may be in asynchronous batch mode or synchronous transactional mode. The general sequence of events is the same for synchronous or asynchronous, with the difference being in the timing of imports, exports and response messages, as defined by DHHR

OP066	3946	1	The solution's data aggregation component should send each provider agency a verified visit report, at least once a calendar day.

The Tellus solution updates in near-real-time, so a provider agency can view a verified visit report through our Administrative Console/Dashboard at any time.

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.

The Tellus solution updates in near-real-time, so a provider agency can view a visit not verified visit report through our Administrative Console/Dashboard at any time.

Solution Backup, Disaster Recovery, and Failover

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.

The database is a critical component of the system. We use Amazon RDS (Relational Database Service) to host our database server. Amazon RDS runs on the same highly reliable infrastructure used by other Amazon Web Services. In production, we provision Multi-AZ database instances.

Amazon RDS synchronously replicates the data to a standby instance in a different Availability Zone (different datacenter). In case of failure of the primary node, Amazon RDS performs an automatic failover to the standby without the need for manual administrative intervention. When a failover is performed, there is a very short period during which the primary node is not accessible. We use many Amazon RDS features that enhance reliability for critical production databases, including automated backups, database snapshots, and automatic host replacement in case of primary database crash. In addition to synchronous replication, database backup snapshots are taken at regular intervals and sent to AWS S3 encrypted storage

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.

Amazon RDS runs on the same highly reliable infrastructure and synchronously replicates the data to a standby instance in a different Availability Zone (different datacenter). RDS features we use to enhance reliability for critical production databases include: automated backups, database snapshots, and automatic host replacement in case of primary database crash. Database backup snapshots are taken at regular intervals and sent to AWS S3 encrypted storage

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.

Tellus EVV performs back-ups during non-peak processing hours. The solution can continue to be used during back-ups.

DR004	4331	1	The solution should support data freezing.

Tellus requires additional information regarding this requirement.

DR005	4261	1	The Vendor should maintain an operational back-up power supply capable of supporting vital functions.

Tellus EVV uses the AWS Government Cloud and runs on fifteen (15) AWS datacenters located in the continental U.S. AWS datacenters are distributed in geographic regions which include clusters of datacenters called Availability Zones. Every region is geographically isolated in terms of power and water supply, and each zone is similarly served by independent networks. Redundantly storing information in different datacenters in multiple regions, availability zones, and datacenters greatly reduces downtime, as the nearest availability zone is activated as a backup when necessary.

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.

Each AWS datacenter is protected by distinct layers of security safeguarding both data and equipment. A layering approach to security helps ensure that failure of one element in the system doesn't create vulnerability in the whole system The Infrastructure Layer comprises energy generators, fire suppression equipment, and ordinary and extraordinary maintenance systems to protect the integrity of the data stored in the datacenter. An Environmental Layer at the locations where AWS datacenters are built are screened for seismic activity and extreme weather, to minimize the risk of structural damage caused by natural occurrences.

DR007	4291	1	The Vendor should equip fire detection and alarm systems with uninterruptable power supply.

Tellus EVV is hosted on AWS cloud.

DR008	4293	1	The Vendor should have a remote backup facility at least one hundred (100) miles away from the primary data center.

The EVV platform is hosted on Amazon Web Services (AWS) Government Cloud and runs on 15 AWS data centers located in the continental U.S. AWS datacenters are distributed in geographic regions that include clusters of datacenters called Availability Zones. Every region is geographically isolated in terms of power and water supply, and each zone is similarly served by independent networks. Redundantly storing information in different datacenters in multiple regions, availability zones and datacenters greatly reduces downtime, as the nearest available node is activated as a backup

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.

Tellus will provide a comprehensive Disaster Recovery and Business Continuity Plan (DR Plan) for this project. The DR Plan will be updated at least annually or any time a major system update or upgrade is performed. The Disaster Recovery Lead will be responsible for updating the entire document and permitted to request information and updates from other employees and departments within the organization to complete this task.

The DR Plan limits service interruptions to a period of 24 hours. However, because our systems are fully utilizing scalability, disaster recovery, high availability and monitoring features of AWS, we do not anticipate that recovery time will be anywhere near 24 hours.

The comprehensive DR Plan will be provided to the Agency when it's modified, or at least

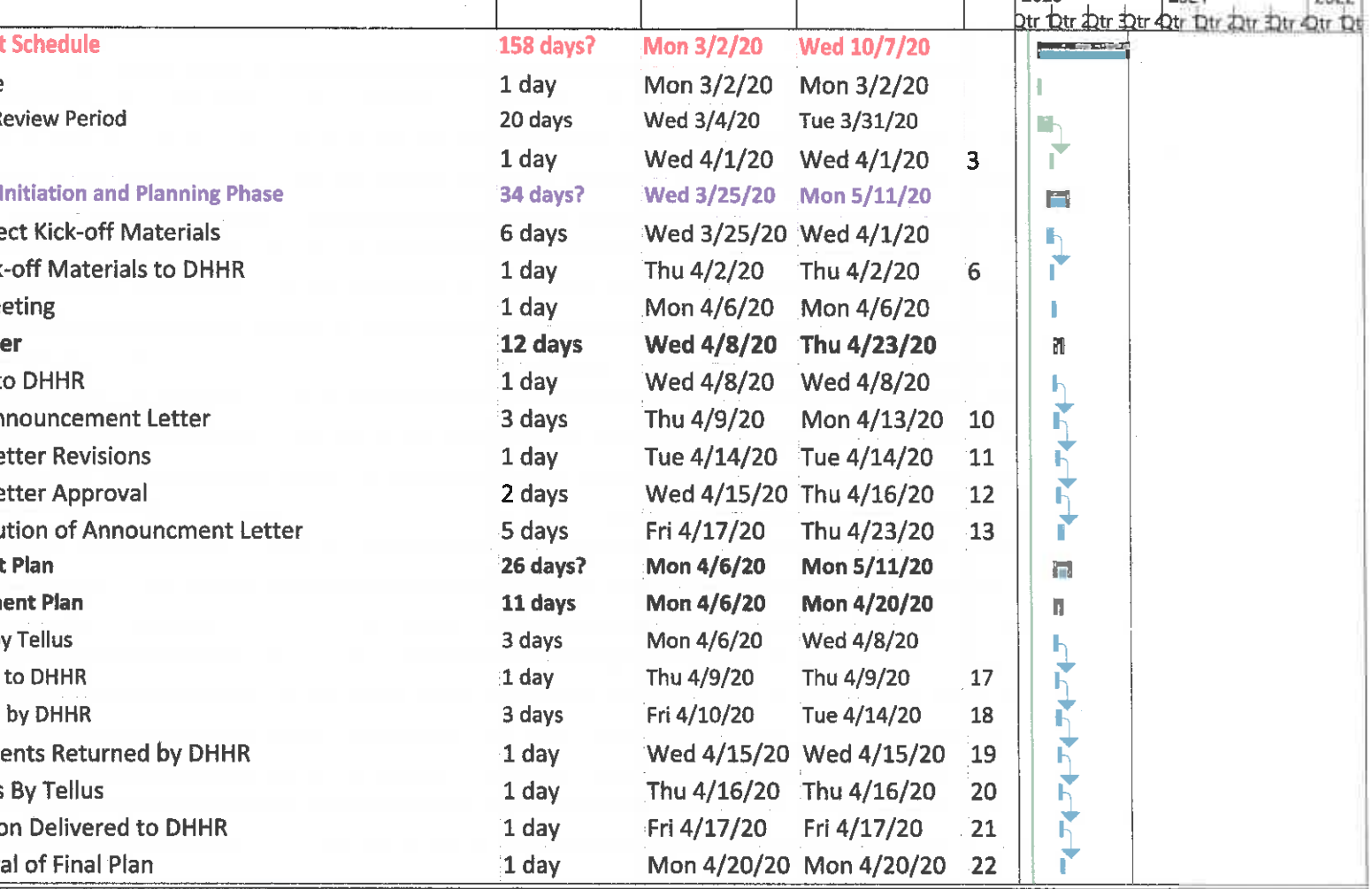
annually, as a PDF file. At the DHHR's request, in accordance to the best interests of the DHHR, the DR Plan will be updated at no additional cost.

The DR Plan will be tested annually or after major infrastructure or system changes to ensure completeness and effectiveness of the existing DR Plan. Results of the testing will be submitted as soon as the test is complete — and at least annually.

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.

All backups and recovery of databases for all cases, including disaster and system failure, are hosted in at least two different availability zones (geographically different data centers). Database instances are kept in sync real-time. Backups are scheduled and occur at regular intervals. They are then encrypted and stored in multiple locations providing 99.9% durability.

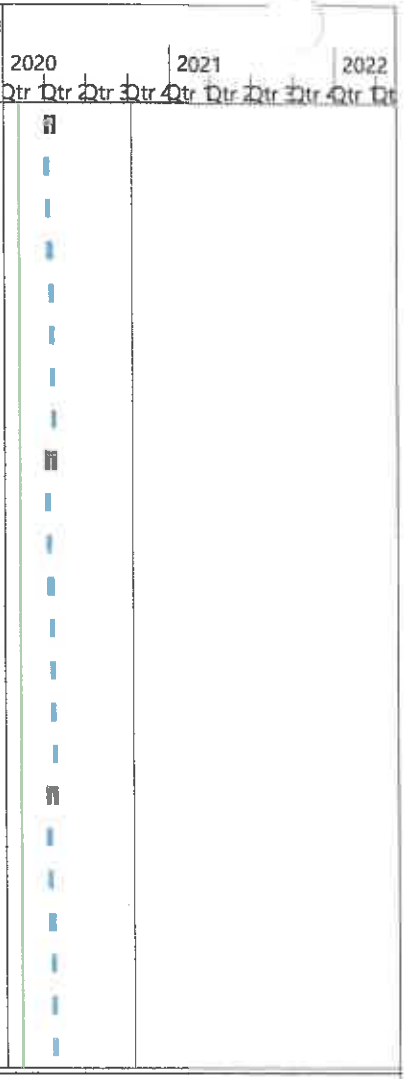
Task N	Du	Start	Finish	Predi
West Virginia Draft Project Schedule	**158 days?**	**Mon 3/2/20**	**Wed 10/7/20**	
Contract Award Made	1 day	Mon 3/2/20	Mon 3/2/20	
Contract Negotiations/Review Period	20 days	Wed 3/4/20	Tue 3/31/20	
Contract Execution	1 day	Wed 4/1/20	Wed 4/1/20	3
Task Group 1 - Project Initiation and Planning Phase	**34 days?**	**Wed 3/25/20**	**Mon 5/11/20**	
Tellus Creates Project Kick-off Materials	6 days	Wed 3/25/20	Wed 4/1/20	
Deliver Project Kick-off Materials to DHHR	1 day	Thu 4/2/20	Thu 4/2/20	6
Project Kick-off Meeting	1 day	Mon 4/6/20	Mon 4/6/20	
Annoucement Letter	**12 days**	**Wed 4/8/20**	**Thu 4/23/20**	
Draft Delivered to DHHR	1 day	Wed 4/8/20	Wed 4/8/20	
DHHR Review Announcement Letter	3 days	Thu 4/9/20	Mon 4/13/20	10
Announcment Letter Revisions	1 day	Tue 4/14/20	Tue 4/14/20	11
Announcment Letter Approval	2 days	Wed 4/15/20	Thu 4/16/20	12
Delivery/Distribution of Announcment Letter	5 days	Fri 4/17/20	Thu 4/23/20	13
Project Management Plan	**26 days?**	**Mon 4/6/20**	**Mon 5/11/20**	
Change Management Plan	**11 days**	**Mon 4/6/20**	**Mon 4/20/20**	
Draft Created by Tellus	3 days	Mon 4/6/20	Wed 4/8/20	
Draft Delivered to DHHR	1 day	Thu 4/9/20	Thu 4/9/20	17
Draft Reviewed by DHHR	3 days	Fri 4/10/20	Tue 4/14/20	18
Marks/Comments Returned by DHHR	1 day	Wed 4/15/20	Wed 4/15/20	19
Plan Revisions By Tellus	1 day	Thu 4/16/20	Thu 4/16/20	20
Revised Version Delivered to DHHR	1 day	Fri 4/17/20	Fri 4/17/20	21
DHHR Approval of Final Plan	1 day	Mon 4/20/20	Mon 4/20/20	22



ct: West Virginia Project
Date: Wed 2/5/2020

Task	Inactive Summary	External Tasks
Split	Manual Task	External Milestone
Milestone	Duration-only	Deadline
Summary	Manual Summary Rollup	Progress
Project Summary	Manual Summary	Manual Progress
Inactive Task	Start-only	
Inactive Milestone	Finish-only	

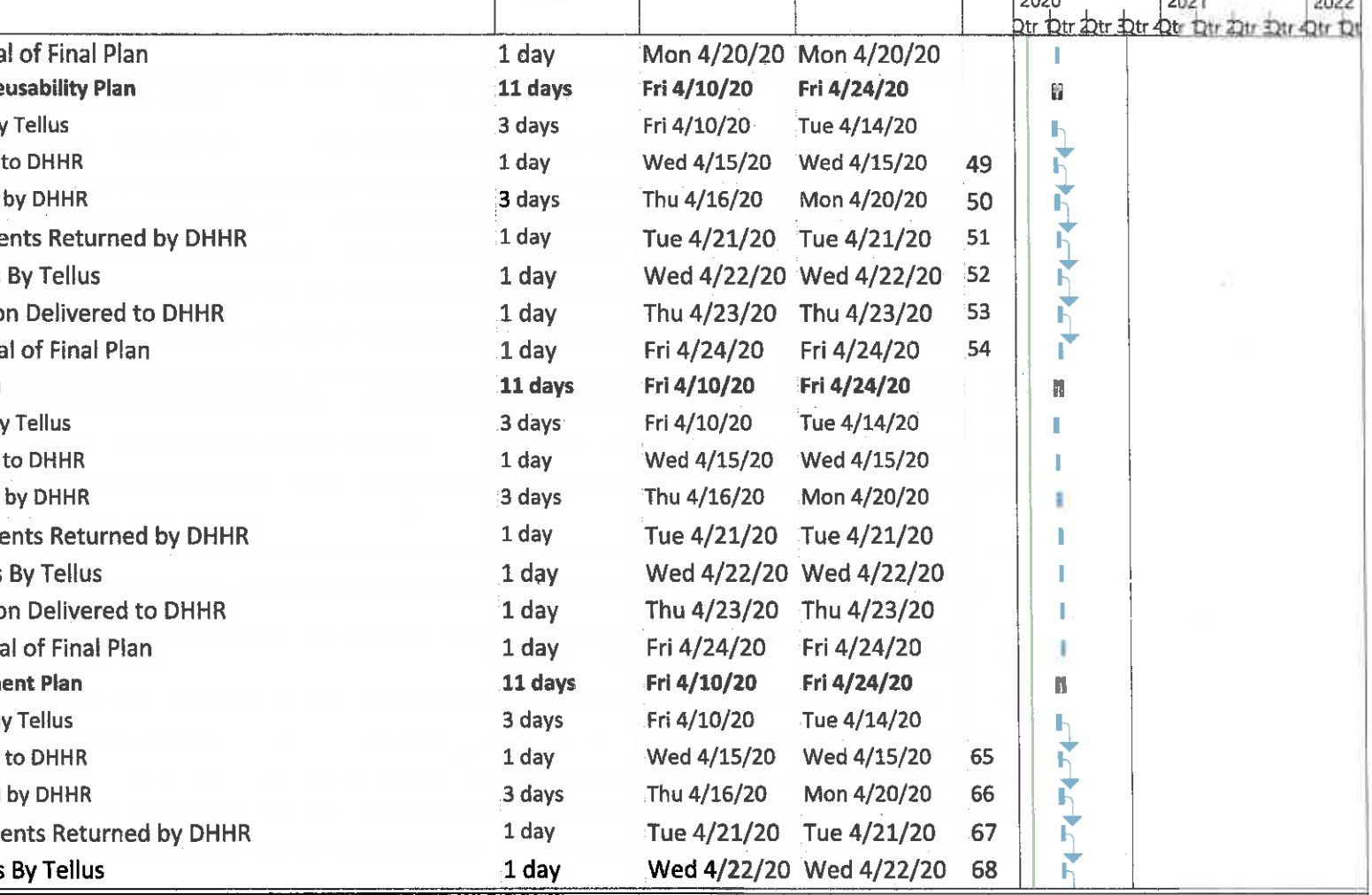
Task N	Du	Start	Finish	Prede
Communication Plan	**11 days**	**Mon 4/6/20**	**Mon 4/20/20**	
Draft Created by Tellus	3 days	Mon 4/6/20	Wed 4/8/20	
Draft Delivered to DHHR	1 day	Thu 4/9/20	Thu 4/9/20	
Draft Reviewed by DHHR	3 days	Fri 4/10/20	Tue 4/14/20	
Marks/Comments Returned by DHHR	1 day	Wed 4/15/20	Wed 4/15/20	
Plan Revisions By Tellus	1 day	Thu 4/16/20	Thu 4/16/20	
Revised Version Delivered to DHHR	1 day	Fri 4/17/20	Fri 4/17/20	
DHHR Approval of Final Plan	1 day	Mon 4/20/20	Mon 4/20/20	
Cost Management Plan	**11 days**	**Mon 4/6/20**	**Mon 4/20/20**	
Draft Created by Tellus	3 days	Mon 4/6/20	Wed 4/8/20	
Draft Delivered to DHHR	1 day	Thu 4/9/20	Thu 4/9/20	
Draft Reviewed by DHHR	3 days	Fri 4/10/20	Tue 4/14/20	
Marks/Comments Returned by DHHR	1 day	Wed 4/15/20	Wed 4/15/20	
Plan Revisions By Tellus	1 day	Thu 4/16/20	Thu 4/16/20	
Revised Version Delivered to DHHR	1 day	Fri 4/17/20	Fri 4/17/20	
DHHR Approval of Final Plan	1 day	Mon 4/20/20	Mon 4/20/20	
Documentation Management Plan	**11 days**	**Mon 4/6/20**	**Mon 4/20/20**	
Draft Created by Tellus	3 days	Mon 4/6/20	Wed 4/8/20	
Draft Delivered to DHHR	1 day	Thu 4/9/20	Thu 4/9/20	
Draft Reviewed by DHHR	3 days	Fri 4/10/20	Tue 4/14/20	
Marks/Comments Returned by DHHR	1 day	Wed 4/15/20	Wed 4/15/20	
Plan Revisions By Tellus	1 day	Thu 4/16/20	Thu 4/16/20	
Revised Version Delivered to DHHR	1 day	Fri 4/17/20	Fri 4/17/20	



ct: West Virginia Project
Date: Wed 2/5/20

Task		Inactive Summary		External Tasks	
Split		Manual Task		External Milestone	
Milestone		Duration-only		Deadline	
Summary		Manual Summary Rollup		Progress	
Project Summary		Manual Summary		Manual Progress	
Inactive Task		Start-only			
Inactive Milestone		Finish-only			

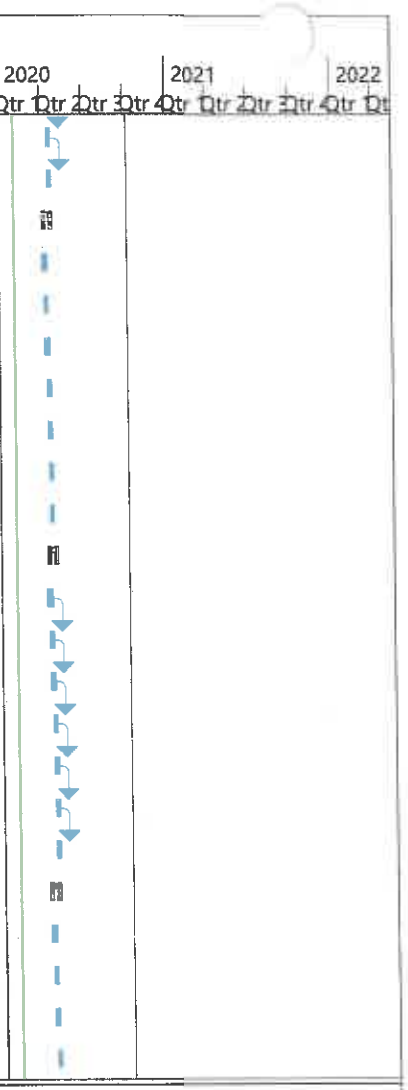
Task Name	Duration	Start	Finish	Predecessors
DHHR Approval of Final Plan	1 day	Mon 4/20/20	Mon 4/20/20	
Modularity and Reusability Plan	**11 days**	**Fri 4/10/20**	**Fri 4/24/20**	
Draft Created by Tellus	3 days	Fri 4/10/20	Tue 4/14/20	
Draft Delivered to DHHR	1 day	Wed 4/15/20	Wed 4/15/20	49
Draft Reviewed by DHHR	3 days	Thu 4/16/20	Mon 4/20/20	50
Marks/Comments Returned by DHHR	1 day	Tue 4/21/20	Tue 4/21/20	51
Plan Revisions By Tellus	1 day	Wed 4/22/20	Wed 4/22/20	52
Revised Version Delivered to DHHR	1 day	Thu 4/23/20	Thu 4/23/20	53
DHHR Approval of Final Plan	1 day	Fri 4/24/20	Fri 4/24/20	54
Project Work Plan	**11 days**	**Fri 4/10/20**	**Fri 4/24/20**	
Draft Created by Tellus	3 days	Fri 4/10/20	Tue 4/14/20	
Draft Delivered to DHHR	1 day	Wed 4/15/20	Wed 4/15/20	
Draft Reviewed by DHHR	3 days	Thu 4/16/20	Mon 4/20/20	
Marks/Comments Returned by DHHR	1 day	Tue 4/21/20	Tue 4/21/20	
Plan Revisions By Tellus	1 day	Wed 4/22/20	Wed 4/22/20	
Revised Version Delivered to DHHR	1 day	Thu 4/23/20	Thu 4/23/20	
DHHR Approval of Final Plan	1 day	Fri 4/24/20	Fri 4/24/20	
Quality Management Plan	**11 days**	**Fri 4/10/20**	**Fri 4/24/20**	
Draft Created by Tellus	3 days	Fri 4/10/20	Tue 4/14/20	
Draft Delivered to DHHR	1 day	Wed 4/15/20	Wed 4/15/20	65
Draft Reviewed by DHHR	3 days	Thu 4/16/20	Mon 4/20/20	66
Marks/Comments Returned by DHHR	1 day	Tue 4/21/20	Tue 4/21/20	67
Plan Revisions By Tellus	1 day	Wed 4/22/20	Wed 4/22/20	68



ct: West Virginia Project
Date: Wed 2/5/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

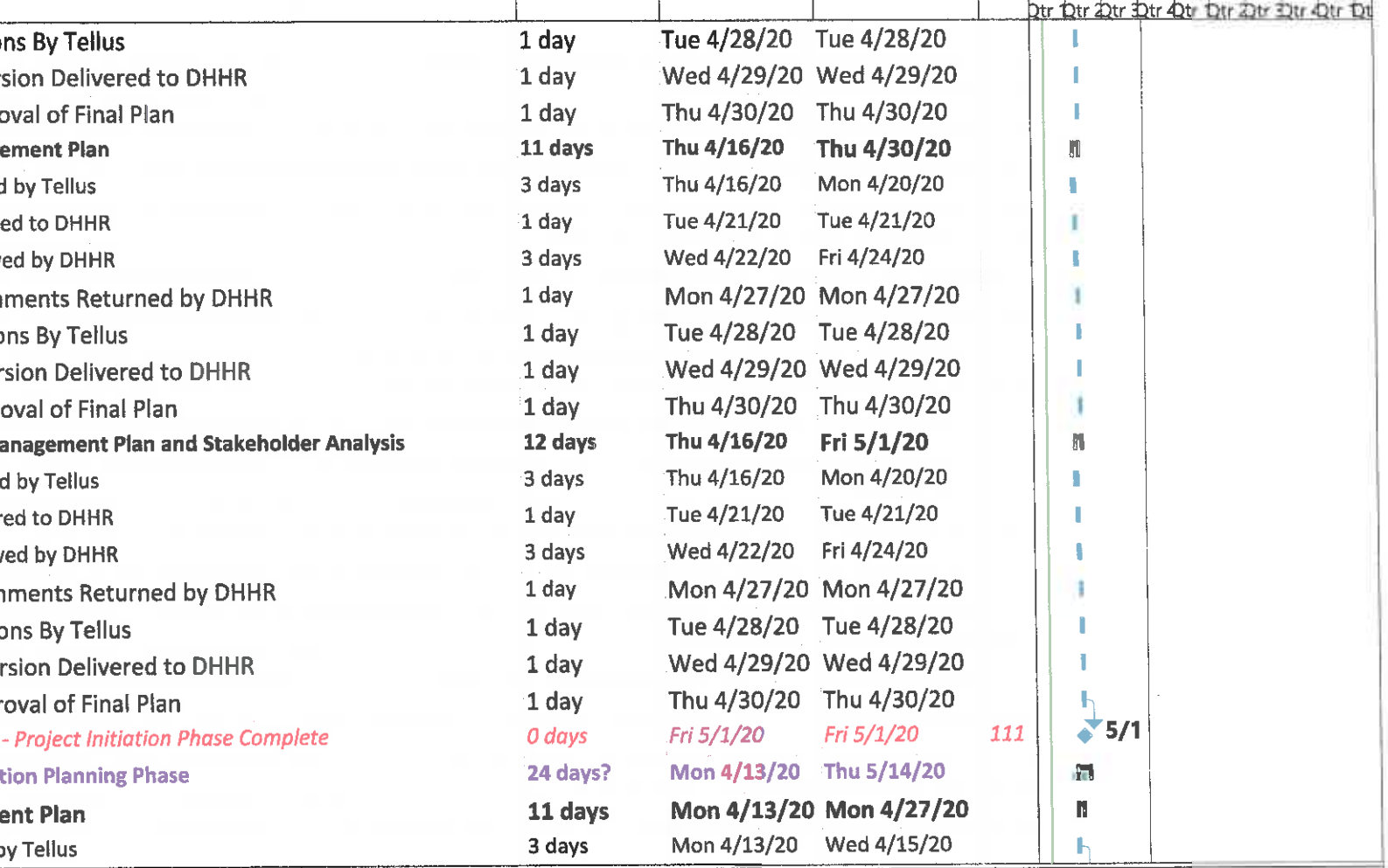
Task N	Du	Start	Finish	Prede
Revised Version Delivered to DHHR	1 day	Thu 4/23/20	Thu 4/23/20	69
DHHR Approval of Final Plan	1 day	Fri 4/24/20	Fri 4/24/20	70
Risk and Issues Management Plan	**11 days**	**Fri 4/10/20**	**Fri 4/24/20**	
Draft Created by Tellus	3 days	Fri 4/10/20	Tue 4/14/20	
Draft Delivered to DHHR	1 day	Wed 4/15/20	Wed 4/15/20	
Draft Reviewed by DHHR	3 days	Thu 4/16/20	Mon 4/20/20	
Marks/Comments Returned by DHHR	1 day	Tue 4/21/20	Tue 4/21/20	
Plan Revisions By Tellus	1 day	Wed 4/22/20	Wed 4/22/20	
Revised Version Delivered to DHHR	1 day	Thu 4/23/20	Thu 4/23/20	
DHHR Approval of Final Plan	1 day	Fri 4/24/20	Fri 4/24/20	
Schedule Management Plan	**11 days**	**Thu 4/16/20**	**Thu 4/30/20**	
Draft Created by Tellus	3 days	Thu 4/16/20	Mon 4/20/20	
Draft Delivered to DHHR	1 day	Tue 4/21/20	Tue 4/21/20	81
Draft Reviewed by DHHR	3 days	Wed 4/22/20	Fri 4/24/20	82
Marks/Comments Returned by DHHR	1 day	Mon 4/27/20	Mon 4/27/20	83
Plan Revisions By Tellus	1 day	Tue 4/28/20	Tue 4/28/20	84
Revised Version Delivered to DHHR	1 day	Wed 4/29/20	Wed 4/29/20	85
DHHR Approval of Final Plan	1 day	Thu 4/30/20	Thu 4/30/20	86
Scope Management Plan	**11 days**	**Thu 4/16/20**	**Thu 4/30/20**	
Draft Created by Tellus	3 days	Thu 4/16/20	Mon 4/20/20	
Draft Delivered to DHHR	1 day	Tue 4/21/20	Tue 4/21/20	
Draft Reviewed by DHHR	3 days	Wed 4/22/20	Fri 4/24/20	
Marks/Comments Returned by DHHR	1 day	Mon 4/27/20	Mon 4/27/20	



ect: West Virginia Project
Date: Wed 2/5/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

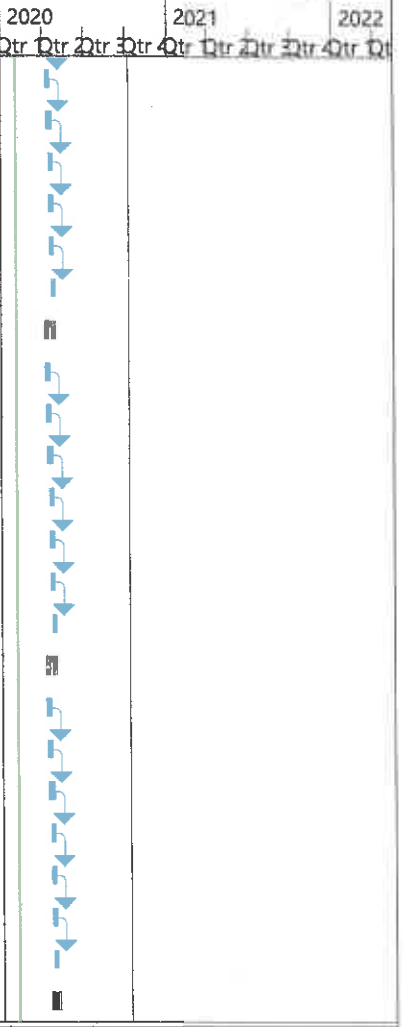
Task N	Du	Start	Finish	Prede
Plan Revisions By Tellus	1 day	Tue 4/28/20	Tue 4/28/20	
Revised Version Delivered to DHHR	1 day	Wed 4/29/20	Wed 4/29/20	
DHHR Approval of Final Plan	1 day	Thu 4/30/20	Thu 4/30/20	
Staffing Management Plan	**11 days**	**Thu 4/16/20**	**Thu 4/30/20**	
Draft Created by Tellus	3 days	Thu 4/16/20	Mon 4/20/20	
Draft Delivered to DHHR	1 day	Tue 4/21/20	Tue 4/21/20	
Draft Reviewed by DHHR	3 days	Wed 4/22/20	Fri 4/24/20	
Marks/Comments Returned by DHHR	1 day	Mon 4/27/20	Mon 4/27/20	
Plan Revisions By Tellus	1 day	Tue 4/28/20	Tue 4/28/20	
Revised Version Delivered to DHHR	1 day	Wed 4/29/20	Wed 4/29/20	
DHHR Approval of Final Plan	1 day	Thu 4/30/20	Thu 4/30/20	
Stakeholder Management Plan and Stakeholder Analysis	**12 days**	**Thu 4/16/20**	**Fri 5/1/20**	
Draft Created by Tellus	3 days	Thu 4/16/20	Mon 4/20/20	
Draft Delivered to DHHR	1 day	Tue 4/21/20	Tue 4/21/20	
Draft Reviewed by DHHR	3 days	Wed 4/22/20	Fri 4/24/20	
Marks/Comments Returned by DHHR	1 day	Mon 4/27/20	Mon 4/27/20	
Plan Revisions By Tellus	1 day	Tue 4/28/20	Tue 4/28/20	
Revised Version Delivered to DHHR	1 day	Wed 4/29/20	Wed 4/29/20	
DHHR Approval of Final Plan	1 day	Thu 4/30/20	Thu 4/30/20	
Milestone 1 - Project Initiation Phase Complete	*0 days*	*Fri 5/1/20*	*Fri 5/1/20*	*111*
Task Group 2 - Solution Planning Phase	**24 days?**	**Mon 4/13/20**	**Thu 5/14/20**	
Data Management Plan	**11 days**	**Mon 4/13/20**	**Mon 4/27/20**	
Draft Created by Tellus	3 days	Mon 4/13/20	Wed 4/15/20	



ect: West Virginia Project
Date: Wed 2/5/20

Task	Inactive Summary	External Tasks
Split	Manual Task	External Milestone
Milestone	Duration-only	Deadline
Summary	Manual Summary Rollup	Progress
Project Summary	Manual Summary	Manual Progress
Inactive Task	Start-only	
Inactive Milestone	Finish-only	

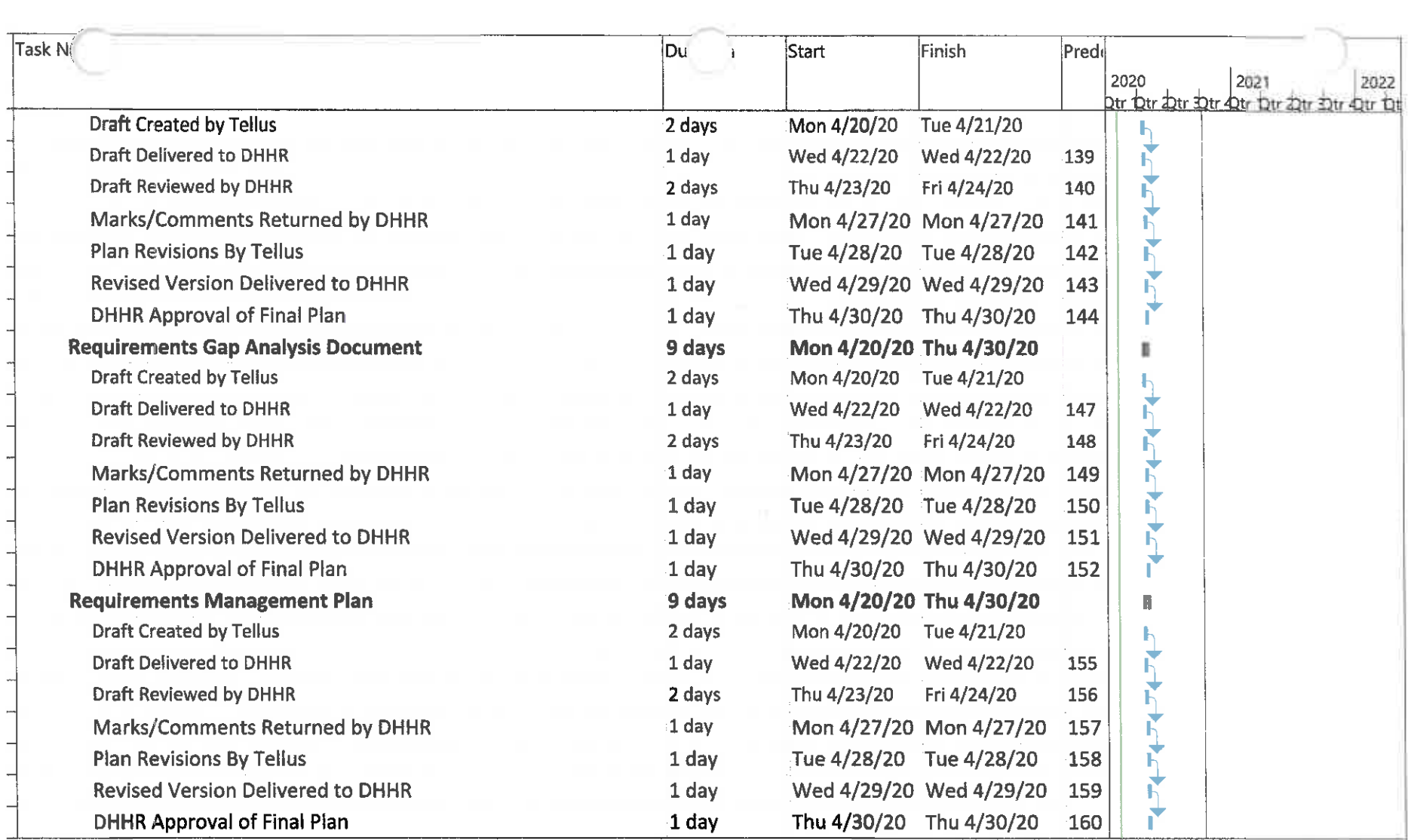
Task N	Du	Start	Finish	Prede
Draft Delivered to DHHR	1 day	Thu 4/16/20	Thu 4/16/20	115
Draft Reviewed by DHHR	3 days	Fri 4/17/20	Tue 4/21/20	116
Marks/Comments Returned by DHHR	1 day	Wed 4/22/20	Wed 4/22/20	117
Plan Revisions By Tellus	1 day	Thu 4/23/20	Thu 4/23/20	118
Revised Version Delivered to DHHR	1 day	Fri 4/24/20	Fri 4/24/20	119
DHHR Approval of Final Plan	1 day	Mon 4/27/20	Mon 4/27/20	120
Data Security, Privacy, and Confidentiality Plan	**11 days**	**Mon 4/13/20**	**Mon 4/27/20**	
Draft Created by Tellus	3 days	Mon 4/13/20	Wed 4/15/20	
Draft Delivered to DHHR	1 day	Thu 4/16/20	Thu 4/16/20	123
Draft Reviewed by DHHR	3 days	Fri 4/17/20	Tue 4/21/20	124
Marks/Comments Returned by DHHR	1 day	Wed 4/22/20	Wed 4/22/20	125
Plan Revisions By Tellus	1 day	Thu 4/23/20	Thu 4/23/20	126
Revised Version Delivered to DHHR	1 day	Fri 4/24/20	Fri 4/24/20	127
DHHR Approval of Final Plan	1 day	Mon 4/27/20	Mon 4/27/20	128
Incident Management Plan	**11 days**	**Mon 4/13/20**	**Mon 4/27/20**	
Draft Created by Tellus	3 days	Mon 4/13/20	Wed 4/15/20	
Draft Delivered to DHHR	1 day	Thu 4/16/20	Thu 4/16/20	131
Draft Reviewed by DHHR	3 days	Fri 4/17/20	Tue 4/21/20	132
Marks/Comments Returned by DHHR	1 day	Wed 4/22/20	Wed 4/22/20	133
Plan Revisions By Tellus	1 day	Thu 4/23/20	Thu 4/23/20	134
Revised Version Delivered to DHHR	1 day	Fri 4/24/20	Fri 4/24/20	135
DHHR Approval of Final Plan	1 day	Mon 4/27/20	Mon 4/27/20	136
Privacy Impact Analysis	**9 days**	**Mon 4/20/20**	**Thu 4/30/20**	



ect: West Virginia Project
Date: Wed 2/5/20

Task	Inactive Summary	External Tasks
Split	Manual Task	External Milestone
Milestone	Duration-only	Deadline
Summary	Manual Summary Rollup	Progress
Project Summary	Manual Summary	Manual Progress
Inactive Task	Start-only	
Inactive Milestone	Finish-only	

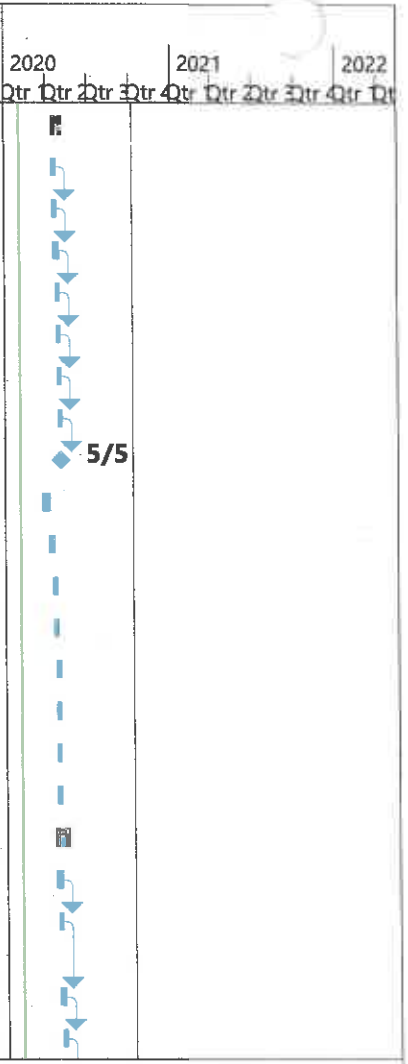
Task N	Du	Start	Finish	Pred
Draft Created by Tellus	2 days	Mon 4/20/20	Tue 4/21/20	
Draft Delivered to DHHR	1 day	Wed 4/22/20	Wed 4/22/20	139
Draft Reviewed by DHHR	2 days	Thu 4/23/20	Fri 4/24/20	140
Marks/Comments Returned by DHHR	1 day	Mon 4/27/20	Mon 4/27/20	141
Plan Revisions By Tellus	1 day	Tue 4/28/20	Tue 4/28/20	142
Revised Version Delivered to DHHR	1 day	Wed 4/29/20	Wed 4/29/20	143
DHHR Approval of Final Plan	1 day	Thu 4/30/20	Thu 4/30/20	144
Requirements Gap Analysis Document	**9 days**	**Mon 4/20/20**	**Thu 4/30/20**	
Draft Created by Tellus	2 days	Mon 4/20/20	Tue 4/21/20	
Draft Delivered to DHHR	1 day	Wed 4/22/20	Wed 4/22/20	147
Draft Reviewed by DHHR	2 days	Thu 4/23/20	Fri 4/24/20	148
Marks/Comments Returned by DHHR	1 day	Mon 4/27/20	Mon 4/27/20	149
Plan Revisions By Tellus	1 day	Tue 4/28/20	Tue 4/28/20	150
Revised Version Delivered to DHHR	1 day	Wed 4/29/20	Wed 4/29/20	151
DHHR Approval of Final Plan	1 day	Thu 4/30/20	Thu 4/30/20	152
Requirements Management Plan	**9 days**	**Mon 4/20/20**	**Thu 4/30/20**	
Draft Created by Tellus	2 days	Mon 4/20/20	Tue 4/21/20	
Draft Delivered to DHHR	1 day	Wed 4/22/20	Wed 4/22/20	155
Draft Reviewed by DHHR	2 days	Thu 4/23/20	Fri 4/24/20	156
Marks/Comments Returned by DHHR	1 day	Mon 4/27/20	Mon 4/27/20	157
Plan Revisions By Tellus	1 day	Tue 4/28/20	Tue 4/28/20	158
Revised Version Delivered to DHHR	1 day	Wed 4/29/20	Wed 4/29/20	159
DHHR Approval of Final Plan	1 day	Thu 4/30/20	Thu 4/30/20	160



ct: West Virginia Project
Date: Wed 2/5/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

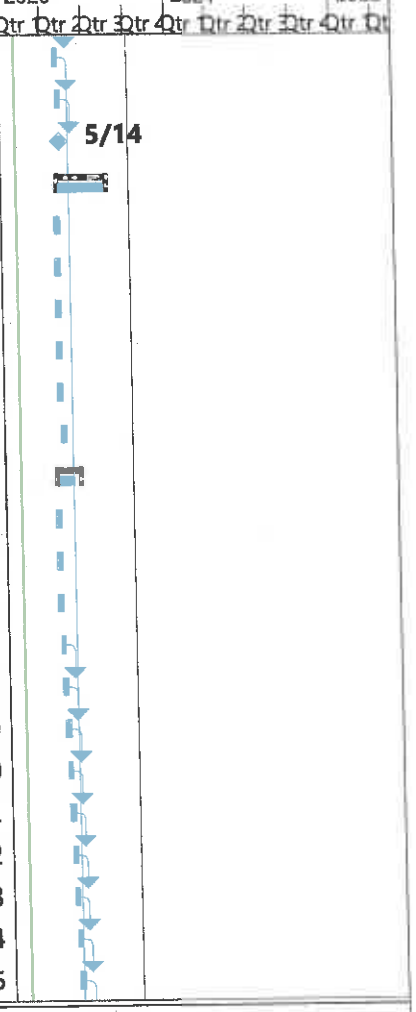
Task Name	Duration	Start	Finish	Predecessors
Master Test Plan (Testing Management Plan)	**11 days**	**Mon 4/20/20**	**Mon 5/4/20**	
Draft Created by Tellus	3 days	Mon 4/20/20	Wed 4/22/20	
Draft Delivered to DHHR	1 day	Thu 4/23/20	Thu 4/23/20	163
Draft Reviewed by DHHR	3 days	Fri 4/24/20	Tue 4/28/20	164
Marks/Comments Returned by DHHR	1 day	Wed 4/29/20	Wed 4/29/20	165
Plan Revisions By Tellus	1 day	Thu 4/30/20	Thu 4/30/20	166
Revised Version Delivered to DHHR	1 day	Fri 5/1/20	Fri 5/1/20	167
DHHR Approval of Final Plan	1 day	Mon 5/4/20	Mon 5/4/20	168
Milestone 2 - Solution Planning 1 Complete	*0 days*	*Tue 5/5/20*	*Tue 5/5/20*	*169*
Secure Training Locations	7 days	Mon 3/30/20	Tue 4/7/20	
Joint Application Development (JAD) session 1 (on-site)	4 days	Mon 4/13/20	Thu 4/16/20	
Joint Application Development (JAD) session 2 (virtual)	1 day	Tue 4/21/20	Tue 4/21/20	
Joint Application Development (JAD) session 3 (virtual)	1 day	Thu 4/23/20	Thu 4/23/20	
Requirements Traceability Matrix Delivered to DHHR	1 day	Tue 4/28/20	Tue 4/28/20	
Safeguard Procedure Report Delivered to DHHR	1 day	Tue 4/28/20	Tue 4/28/20	
Security Plan	1 day	Tue 4/28/20	Tue 4/28/20	
System Backup and Record Retention Plan	1 day	Tue 4/28/20	Tue 4/28/20	
Requirements Specification Document	**15 days**	**Fri 4/24/20**	**Thu 5/14/20**	
Requirements Specification Document Draft	3 days	Fri 4/24/20	Tue 4/28/20	
Requirements Specification Document Delivered to DHHR for Review	1 day	Wed 4/29/20	Wed 4/29/20	180
Marks/Comments Returned by DHHR for RSD	3 days	Thu 4/30/20	Mon 5/4/20	181
Tellus Revision of RSD	2 days	Tue 5/5/20	Wed 5/6/20	182

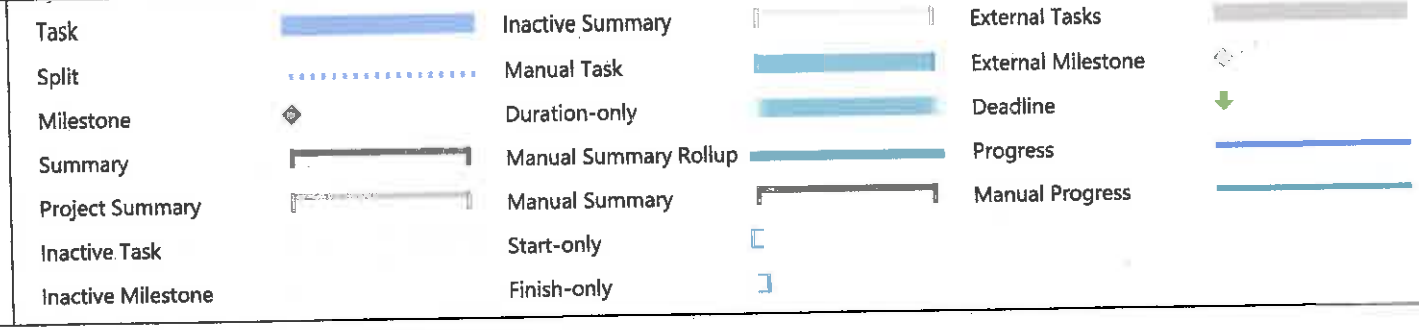


ect: West Virginia Project
Date: Wed 2/5/20

Task	Inactive Summary	External Tasks
Split	Manual Task	External Milestone
Milestone	Duration-only	Deadline
Summary	Manual Summary Rollup	Progress
Project Summary	Manual Summary	Manual Progress
Inactive Task	Start-only	
Inactive Milestone	Finish-only	

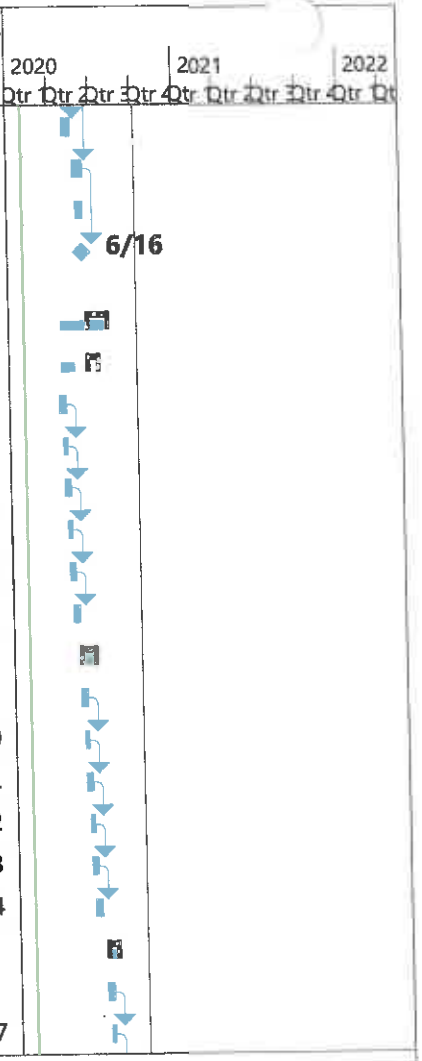
Task N	Du	Start	Finish	Prede
DHHR Approval/Sign-off of Requirements Specifications Docum	2 days	Thu 5/7/20	Fri 5/8/20	183
System Requirement Document/Backlog User Stories or Use Case	3 days	Mon 5/11/20	Wed 5/13/20	184
Milestone 3 - Solution Planning 2 Complete	*0 days*	*Thu 5/14/20*	*Thu 5/14/20*	*185*
Task Group 3 - Solution Design, Testing, and Operational Readiness	**78 days**	**Mon 5/4/20**	**Wed 8/19/20**	
Diaster Recovery and Business Continuity Plan	5 days	Mon 5/4/20	Fri 5/8/20	
Database Design Document and Data Models	5 days	Mon 5/4/20	Fri 5/8/20	
Detailed System Design Document	5 days	Mon 5/4/20	Fri 5/8/20	
Capacity Plan	5 days	Mon 5/4/20	Fri 5/8/20	
Configuration Management Plan	5 days	Mon 5/4/20	Fri 5/8/20	
Data Conversion Plan	5 days	Mon 5/11/20	Fri 5/15/20	
Integration Tasks	**37 days**	Mon 4/27/20	Tue 6/16/20	
SFTP Setup	5 days	Mon 4/27/20	Fri 5/1/20	
Channel Configuration	5 days	Mon 4/27/20	Fri 5/1/20	
Database Setup	5 days	Mon 4/27/20	Fri 5/1/20	
PA, Member, Provider Sample File Deliveried to Tellus - Cycle 1	1 day	Mon 5/4/20	Mon 5/4/20	
PA, Member, Provider Sample File Results to DHHR - Cycle 1	3 days	Tue 5/5/20	Thu 5/7/20	198
PA, Member, Provider File Updates/Corrections - Cycle 1	3 days	Fri 5/8/20	Tue 5/12/20	199
PA, Member, Provider Sample File Deliveried to Tellus - Cycle 2	1 day	Wed 5/13/20	Wed 5/13/20	200
PA, Member, Provider Sample File Results to DHHR - Cycle 2	3 days	Thu 5/14/20	Mon 5/18/20	201
PA, Member, Provider File Updates/Corrections - Cycle 2	3 days	Tue 5/19/20	Thu 5/21/20	202
PA, Member, Provider Sample File Deliveried to Tellus - Cycle 3	1 day	Fri 5/22/20	Fri 5/22/20	203
PA, Member, Provider Sample File Results to DHHR - Cycle 3	3 days	Mon 5/25/20	Wed 5/27/20	204
PA, Member, Provider File Updates/Corrections - Cycle 3	3 days	Thu 5/28/20	Mon 6/1/20	205





ject: West Virginia Project
n Date: Wed 2/5/20

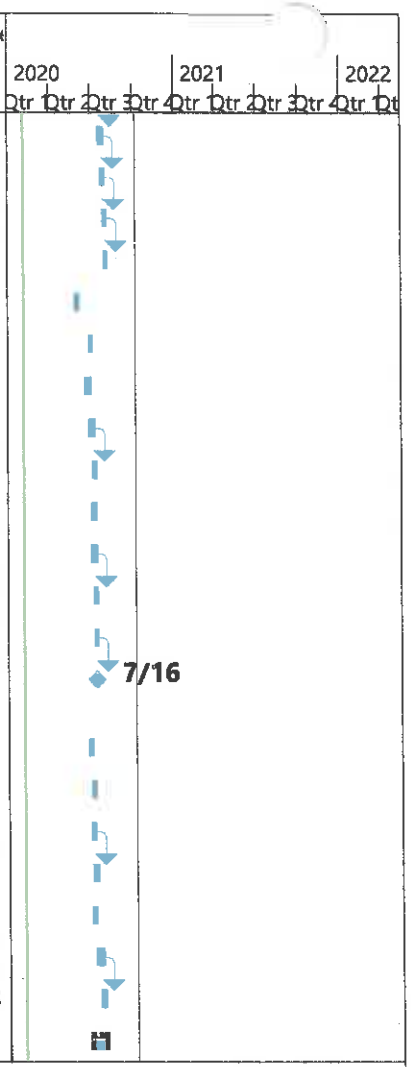
Task N	Du	Start	Finish	Pred
Data Conversion Test Cases	10 days	Mon 5/11/20	Fri 5/22/20	184
Data Conversion Test Results	10 days	Tue 6/2/20	Mon 6/15/20	206
Identify Pilot Providers	6 days	Mon 6/8/20	Mon 6/15/20	
Milestone 4 - Solution Design, Testing, and Operational Readiness 1 Complete	*0 days*	*Tue 6/16/20*	*Tue 6/16/20*	*208*
Outreach and Communications	31 days	Wed 6/24/20	Wed 8/5/20	
Email Blasts #1	**16 days**	**Wed 6/24/20**	**Wed 7/15/20**	
Draft - Email Blast #1	6 days	Mon 4/27/20	Mon 5/4/20	
Deliver - Email Blast #1	1 day	Tue 5/5/20	Tue 5/5/20	213
Review - Email Blast #1	4 days	Wed 5/6/20	Mon 5/11/20	214
Revisions - Email Blast #1	2 days	Tue 5/12/20	Wed 5/13/20	215
Approval - Email Blast #1	3 days	Thu 5/14/20	Mon 5/18/20	216
Distribution - Email Blast #1	6 days	Tue 5/19/20	Tue 5/26/20	217
Email Blasts #2	**22 days**	**Mon 6/1/20**	**Tue 6/30/20**	
Draft - Email Blast #2	6 days	Mon 6/1/20	Mon 6/8/20	
Deliver - Email Blast #2	1 day	Tue 6/9/20	Tue 6/9/20	220
Review - Email Blast #2	4 days	Wed 6/10/20	Mon 6/15/20	221
Revisions - Email Blast #2	2 days	Tue 6/16/20	Wed 6/17/20	222
Approval - Email Blast #2	3 days	Thu 6/18/20	Mon 6/22/20	223
Distribution - Email Blast #2	6 days	Tue 6/23/20	Tue 6/30/20	224
Email Blasts #3	**15 days**	**Thu 7/16/20**	**Wed 8/5/20**	
Draft - Email Blast #3	5 days	Thu 7/16/20	Wed 7/22/20	
Deliver - Email Blast #3	1 day	Thu 7/23/20	Thu 7/23/20	227



ject: West Virginia Project
n Date: Wed 2/5/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

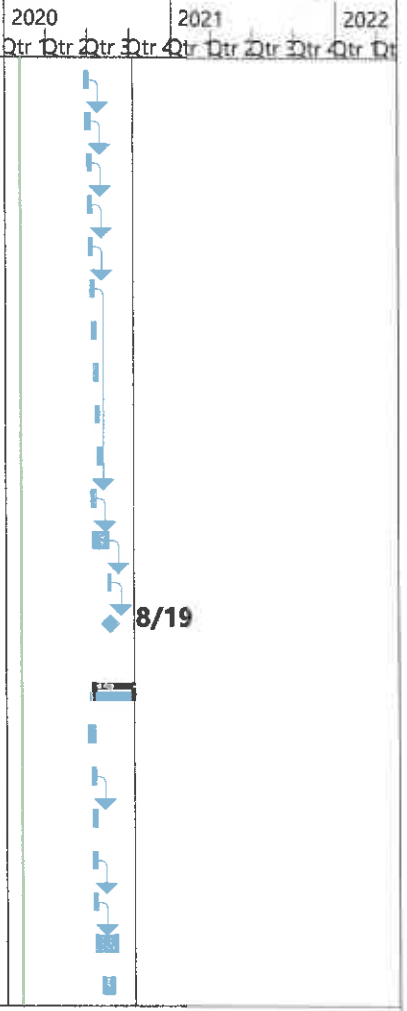
Task N	Du	Start	Finish	Prede
Review - Email Blast #3	3 days	Fri 7/24/20	Tue 7/28/20	228
Revisions - Email Blast #3	3 days	Wed 7/29/20	Fri 7/31/20	229
Approval - Email Blast #3	2 days	Mon 8/3/20	Tue 8/4/20	230
Distribution - Email Blast #3	1 day	Wed 8/5/20	Wed 8/5/20	231
Federal Certification and Review Management Plan	3 days	*Mon 6/1/20*	*Wed 6/3/20*	
Interface Inventory	1 day	Fri 7/3/20	Fri 7/3/20	
Load and Stress Test Cases	4 days	Thu 6/25/20	Tue 6/30/20	
Load and Stress Testing	5 days	Fri 7/3/20	Thu 7/9/20	
Load and Stress Test Results	2 days	Fri 7/10/20	Mon 7/13/20	236
Operational Readiness Plan	4 days	Wed 7/8/20	Mon 7/13/20	
Operational Readiness Test Scripts	4 days	Wed 7/8/20	Mon 7/13/20	
Operational Readiness Test Results	1 day	Tue 7/14/20	Tue 7/14/20	239
System Demonstration	1 day	Wed 7/15/20	Wed 7/15/20	
Milestone 5 - Solution Design, Testing, and Operational Readiness 2 Complete	*0 days*	*Thu 7/16/20*	*Thu 7/16/20*	*241*
Reports and Forms Inventory	1 day	Thu 7/2/20	Thu 7/2/20	
System Integration Plan	3 days	Mon 7/6/20	Wed 7/8/20	
System Integration Test Cases	3 days	Mon 7/6/20	Wed 7/8/20	
System Integration Test Results	3 days	Thu 7/9/20	Mon 7/13/20	245
Regression Test Cases	3 days	Mon 7/6/20	Wed 7/8/20	
Regression Testing	7 days	Wed 7/15/20	Thu 7/23/20	
Regression Test Results	3 days	Fri 7/24/20	Tue 7/28/20	248
Training Management Plan	**22 days**	**Thu 7/2/20**	**Fri 7/31/20**	



ect: West Virginia Project
Date: Wed 2/5/20

Task	Inactive Summary	External Tasks
Split	Manual Task	External Milestone
Milestone	Duration-only	Deadline
Summary	Manual Summary Rollup	Progress
Project Summary	Manual Summary	Manual Progress
Inactive Task	Start-only	
Inactive Milestone	Finish-only	

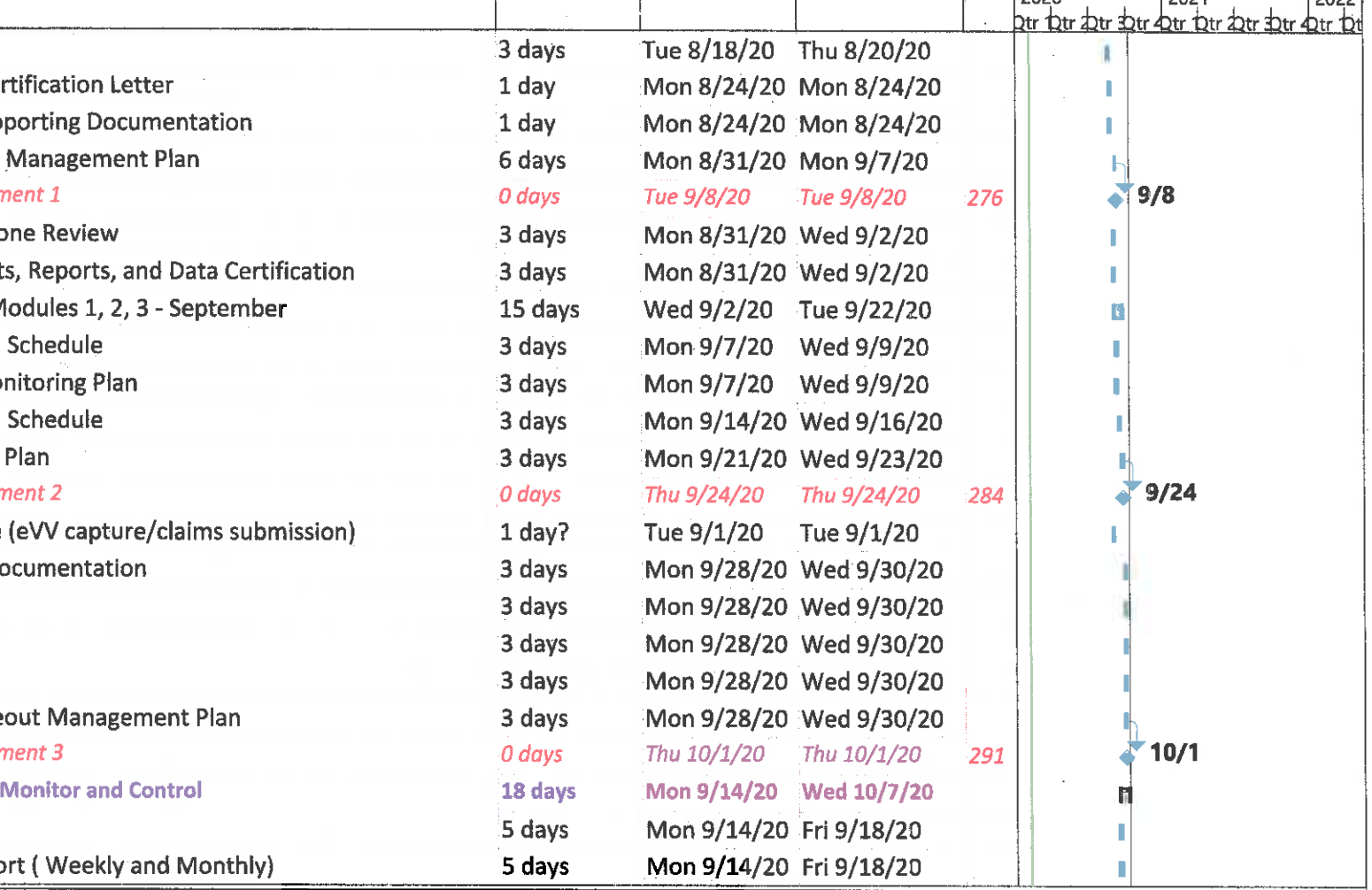
Task N	Du	Start	Finish	Prede
Draft of Training Materials Delivered to DHHR	1 day	Thu 7/2/20	Thu 7/2/20	
Draft Training Materials Reviewed by DHHR	3 days	Fri 7/3/20	Tue 7/7/20	251
Marks/Comments Returned by DHHR	1 day	Wed 7/8/20	Wed 7/8/20	252
Training Materials Plan Revisions By Tellus	1 day	Thu 7/9/20	Thu 7/9/20	253
Revised Version of Training Materials Delivered to DHHR	1 day	Fri 7/10/20	Fri 7/10/20	254
DHHR Approval of Final Training Plan/Materials	1 day	Mon 7/13/20	Mon 7/13/20	255
On-site Training Module 1	2 days	Thu 7/16/20	Fri 7/17/20	
On-site Training Module 2	3 days	Mon 7/20/20	Wed 7/22/20	
On-site Training Module 3	2 days	Thu 7/23/20	Fri 7/24/20	
Webinar Training Modules 1, 2, 3 - July	5 days	Mon 7/27/20	Fri 7/31/20	
User Acceptance Test Cases	3 days	Tue 7/14/20	Thu 7/16/20	256
User Acceptance Testing	20 days	Fri 7/17/20	Thu 8/13/20	261
User Acceptance Test Results and Letter of Completion	3 days	Fri 8/14/20	Tue 8/18/20	262
Milestone 6 - Solution Design, Testing, and Operational Readiness 3 Complete	*0 days*	*Wed 8/19/20*	*Wed 8/19/20*	*263*
Task Group 4 - Solution Deployment	**62 days?**	**Tue 7/14/20**	**Wed 10/7/20**	
Implementation Plan (Rollout Plan)	6 days	Mon 7/6/20	Mon 7/13/20	
Production Environment Setup	1 day	Tue 7/14/20	Tue 7/14/20	
Data Load to Production	3 days	Wed 7/15/20	Fri 7/17/20	267
Production Environment Smoke Test	1 day	Thu 7/16/20	Thu 7/16/20	
System Go-Live	1 day?	Fri 7/17/20	Fri 7/17/20	269
Pilot Providers Begin Logging Visits and Submitting Claims	30 days	Mon 7/20/20	Fri 8/28/20	270
Webinar Training Modules 1, 2, 3 - August	15 days	Mon 8/3/20	Fri 8/21/20	



ect: West Virginia Project
Date: Wed 2/5/20

Task	Inactive Summary	External Tasks
Split	Manual Task	External Milestone
Milestone	Duration-only	Deadline
Summary	Manual Summary Rollup	Progress
Project Summary	Manual Summary	Manual Progress
Inactive Task	Start-only	
Inactive Milestone	Finish-only	

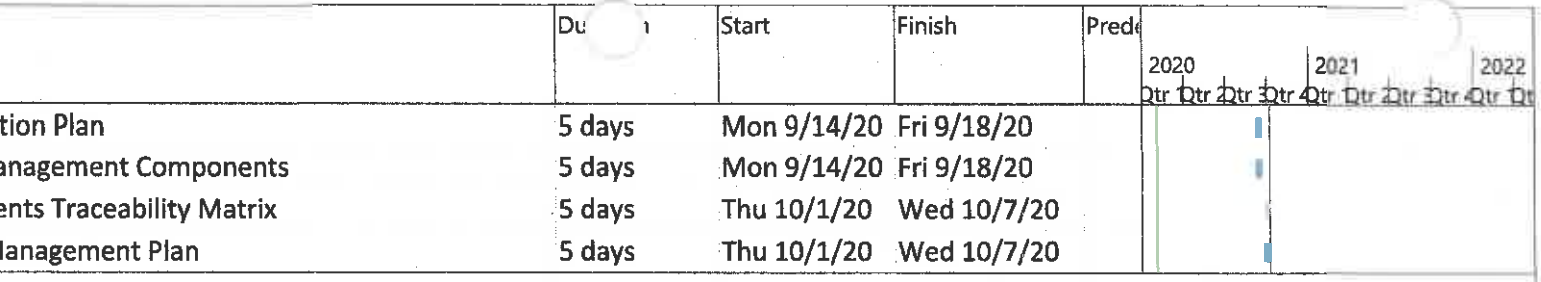
Task Na	Du	Start	Finish	Prede
Cutover Play Book	3 days	Tue 8/18/20	Thu 8/20/20	
Implementation Certification Letter	1 day	Mon 8/24/20	Mon 8/24/20	
Federal Review Supporting Documentation	1 day	Mon 8/24/20	Mon 8/24/20	
Operations Change Management Plan	6 days	Mon 8/31/20	Mon 9/7/20	
Milestone 7 - Deployment 1	*0 days*	*Tue 9/8/20*	*Tue 9/8/20*	*276*
Operational Milestone Review	3 days	Mon 8/31/20	Wed 9/2/20	
Product Screenshots, Reports, and Data Certification	3 days	Mon 8/31/20	Wed 9/2/20	
Webinar Training Modules 1, 2, 3 - September	15 days	Wed 9/2/20	Tue 9/22/20	
Report Distribution Schedule	3 days	Mon 9/7/20	Wed 9/9/20	
Solution Health Monitoring Plan	3 days	Mon 9/7/20	Wed 9/9/20	
Report Distribution Schedule	3 days	Mon 9/14/20	Wed 9/16/20	
System Operations Plan	3 days	Mon 9/21/20	Wed 9/23/20	
Milestone 8 - Deployment 2	*0 days*	*Thu 9/24/20*	*Thu 9/24/20*	*284*
Mandatory Go-Live (eVV capture/claims submission)	1 day?	Tue 9/1/20	Tue 9/1/20	
System and User Documentation	3 days	Mon 9/28/20	Wed 9/30/20	
Training Materials	3 days	Mon 9/28/20	Wed 9/30/20	
Training Report	3 days	Mon 9/28/20	Wed 9/30/20	
Training Schedule	3 days	Mon 9/28/20	Wed 9/30/20	
Turnover and Closeout Management Plan	3 days	Mon 9/28/20	Wed 9/30/20	
Milestone 9 - Deployment 3	*0 days*	*Thu 10/1/20*	*Thu 10/1/20*	*291*
Task Group 5 - Project Monitor and Control	**18 days**	**Mon 9/14/20**	**Wed 10/7/20**	
Project Schedule	5 days	Mon 9/14/20	Fri 9/18/20	
Project Status Report (Weekly and Monthly)	5 days	Mon 9/14/20	Fri 9/18/20	



ct: West Virginia Project
Date: Wed 2/5/20

Task	Inactive Summary	External Tasks
Split	Manual Task	External Milestone
Milestone	Duration-only	Deadline
Summary	Manual Summary Rollup	Progress
Project Summary	Manual Summary	Manual Progress
Inactive Task	Start-only	
Inactive Milestone	Finish-only	

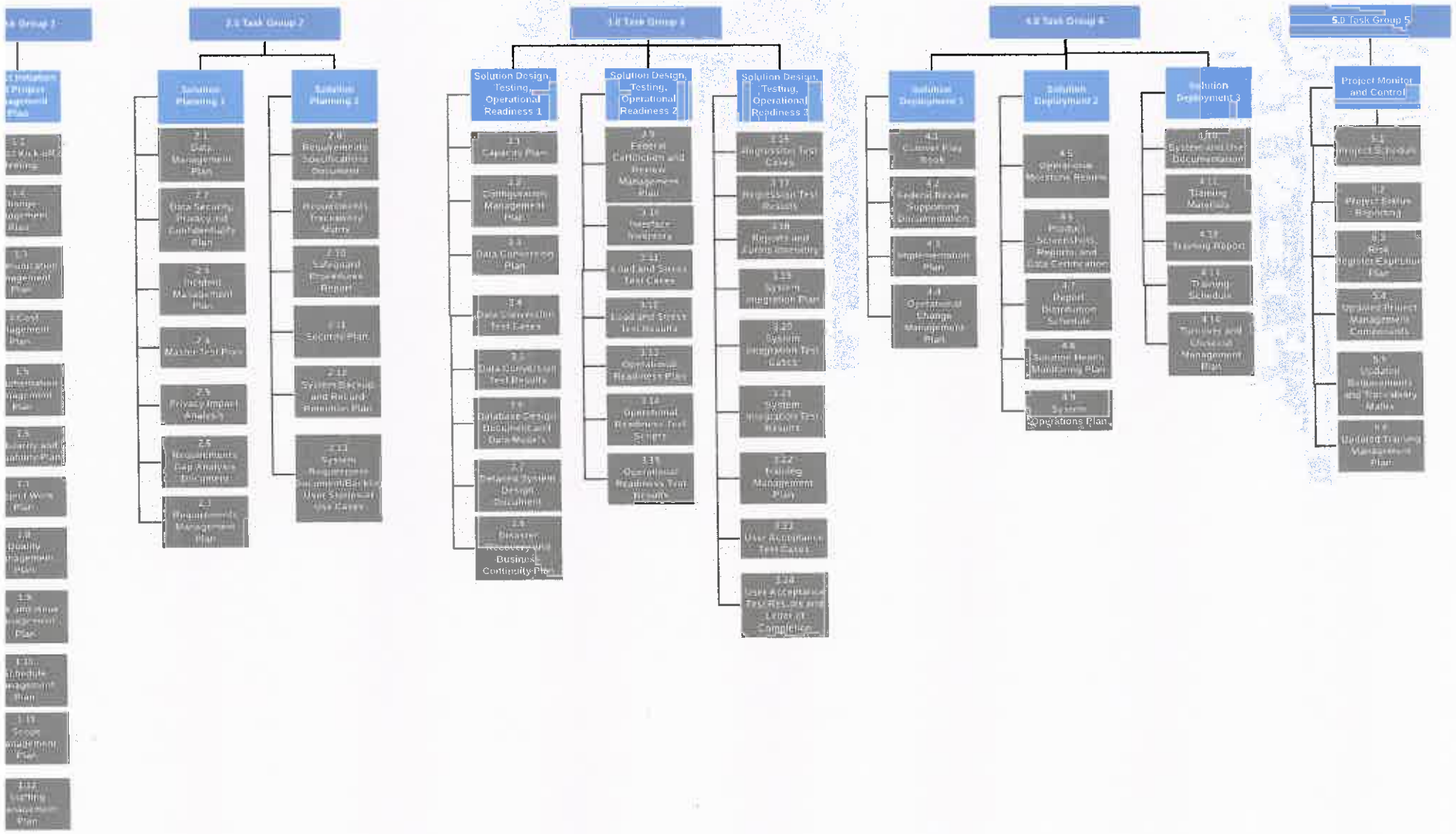
Task N	Du	Start	Finish	Prede
Risk Register/Expection Plan	5 days	Mon 9/14/20	Fri 9/18/20	
Updated Project Management Components	5 days	Mon 9/14/20	Fri 9/18/20	
Updated Requirements Traceability Matrix	5 days	Thu 10/1/20	Wed 10/7/20	
Updated Training Management Plan	5 days	Thu 10/1/20	Wed 10/7/20	



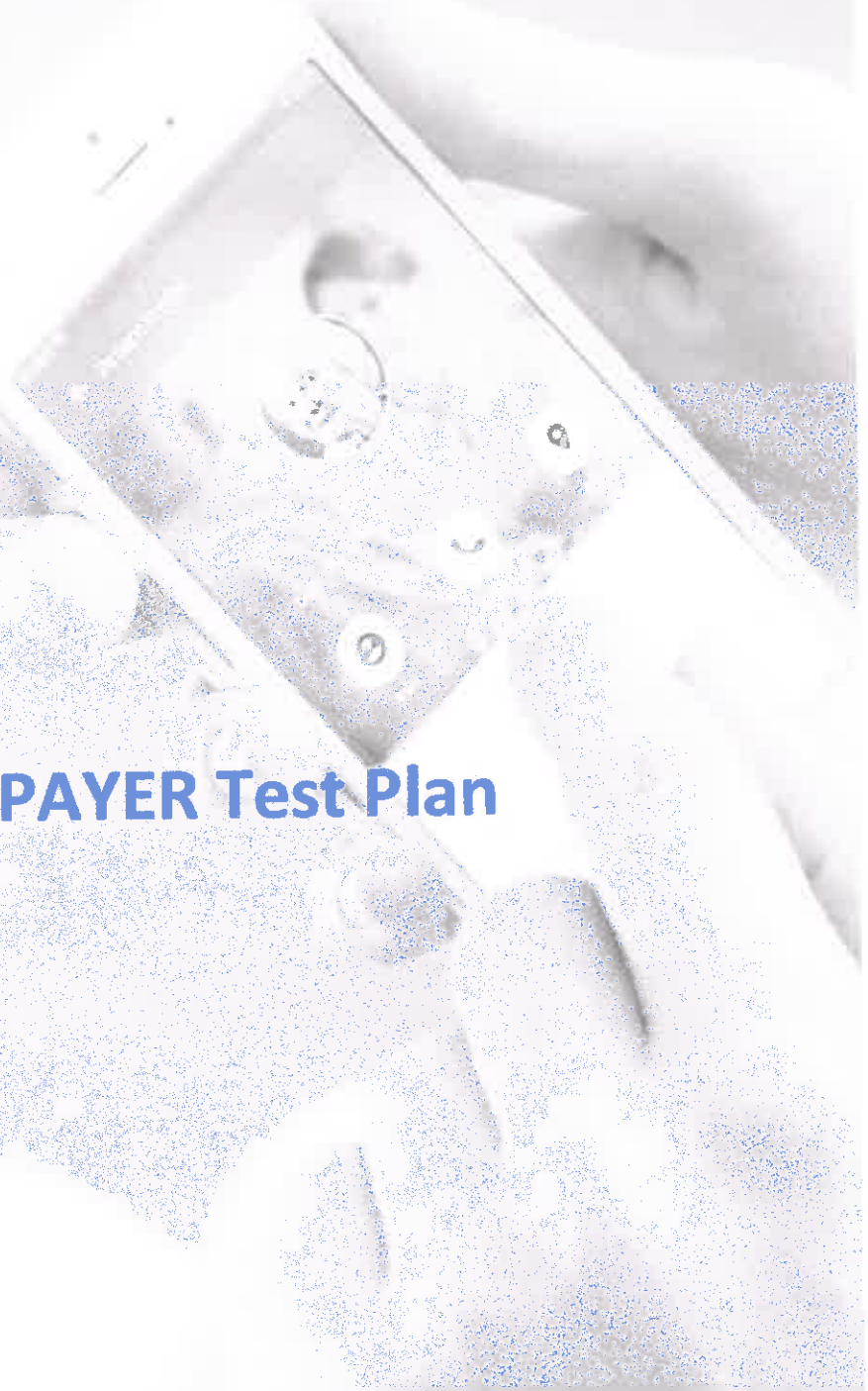
ect: West Virginia Project
Date: Wed 2/5/20

Task	Inactive Summary	External Tasks
Split	Manual Task	External Milestone
Milestone	Duration-only	Deadline
Summary	Manual Summary Rollup	Progress
Project Summary	Manual Summary	Manual Progress
Inactive Task	Start-only	
Inactive Milestone	Finish-only	

West Virginia Electronic Visit Verification Program



TELLUS



PayerNameHere PAYER Test Plan

Revision: 1.1
Date: March 10, 2020

TELLUS, LLC
800 Fairway Drive, #360
Deerfield Beach, FL 33441
(954) 719-0004
www.4tellus.com

STATEMENT OF CONFIDENTIALITY

This document contains confidential and proprietary information of Tellus, LLC ("Tellus") and is supplied to allow the recipient to make an evaluation of Tellus as a candidate for the delivery of software solutions and professional services. The recipient(s) of this document agree to inform present and future employees who receive or have access to this proposal of the confidential nature of this item and to instruct each employee not to disclose any information concerning this document to others without prior written consent from a duly authorized Tellus representative. The recipient further agrees to protect said confidential information as internal confidential information would be protected and not to disclose any information concerning this document to others without prior written consent from a duly authorized Tellus representative. The recipient of this document agrees not to duplicate or permit others to duplicate any material contained hereunder except for internal use.

REVISION HISTORY

NAME	REVISION DATE	VERSION	DESCRIPTION OF CHANGES
			Initial Draft

Table of Contents

1. INTRODUCTION 4
   1.1. REFERENCES & RELATED DOCUMENTS 5
2. PROJECT MANAGEMENT OVERVIEW 5
   2.1. ACTIVITIES BY PHASE 5
   2.2. KEY DELIVERABLES BY PHASE 6
   2.3. ENVIRONMENTS 7
   2.4. PROJECT STAFFING 10
3. TEST SCHEDULE AND GOVERNANCE 10
   3.1. TEST PLANNING 10
   3.2. TEST SCHEDULE 11
   3.3. REQUIRED TESTING RESOURCES 11
   3.4. UAT ENTRANCE CRITERIA 12
   3.5. UAT TEST RELEASE CRITERIA 12
   3.6. REQUIREMENTS TRACEABILITY CONFORMANCE 13
4. TEST STRATEGY 13
   4.1. FUNCTIONAL TEST OBJECTIVES & SCOPE 13
      4.1.1. Prior Authorization (PA) Objectives 13
      4.1.2. Provider Messaging Text Objectives 17
      4.1.3. Recipient Objectives 19
      4.1.4. Claims Messaging Test Objectives 20
      4.1.5. Visit Management Test Objectives 24
5. DEFECT MANAGEMENT 25
6. APPROVALS 26
7. APPENDIX A - ACRONYMS & DEFINITION OF TERMS 27
   7.1. ACRONYMS 27
   7.2. DEFINITION OF TERMS 27

1. INTRODUCTION

This document is the Test Plan for the Payer MCO Integration to the Electronic Visit Verification (eVV) platform. It identifies the project objectives, deliverables, resource requirements and risks associated with managing the testing of this project. Progress will be tracked with the Jira and test coverage metric reports.

The testing program for this integrated solution will address the following functional areas:

1. Prior Authorization (PA) Messaging Test Objectives:
   1.1. Inbound Process New PA.
   1.2. Inbound Additional PA for Recipient - Same PA #.
   1.3. Inbound Additional PA for Recipient - Different PA #.
   1.4. Adjust Existing PA.
   1.5. Error PA - Overlapping Dates.
   1.6. Rejected PA – Missing Required Fields.
2. Provider Messaging Test Objectives:
   2.1. Create New Provider.
   2.2. Update Existing Provider.
   2.3. Make Existing Provider Ineligible.
3. Recipient Messaging Test Objectives:
   3.1. Create New Recipient.
   3.2. Update Existing Recipient.
   3.3. Make Existing Recipient Ineligible.
4. Claims Messaging Test Objectives:
   4.1. Claims Submission via 837P (New Claim) Completed by Tellus.
   4.2. Claims Submission via 837P (New Claim) processed by Payer.
   4.3. Claims Submission via 837P (Void Claim) Completed by Tellus.
   4.4. Claims Submission via 837P (Void Claim) processed by Payer.
   4.5. Claims Submission via 837P (Adjusted Claim) Completed by Tellus.
   4.6. Claims Submission via 837P (Adjusted Claim) processed by Payer.
   4.7. Claims Submission via 837P (Denied Claim Resubmitted) Completed by Tellus.
   4.8. Claims Submission via 837P (Denied Claim Resubmitted) processed by Payer.
   4.9. 999 generated by Payer
   4.10. 277 generated by Payer
   4.11. 835 (or 835 equivalent) generated by Payer
   4.12. 999 Processed by Tellus.
   4.13. 835 Processed by Tellus (Full Payment).
   4.14. 835 Processed by Tellus (Partial Payment).

4.15. 835 Processed by Tellus (Denial).
4.16. Overnight Claim Spanning Midnight.
5. Visit Management Test Objectives
5.1. Overnight Visit
5.2. Multiple Recipients on a Single Visit - No TT Modifier
5.3. Multiple Recipients on a Single Visit - With TT Modifier
5.4. Multiple Service Code on a Single Visit
5.5. GPS Maximum Range between Scheduled and Actual Start
5.6. Completed Late Visit

1.1. REFERENCES & RELATED DOCUMENTS

Table 1: Related Documents

DOCUMENT TITLE	DOCUMENT NO.	REVISION
Tellus eVV Payer Implementation Guide		
Payer Integration Specification		
Payer UAT - Inbound Provider File Validation		
Payer UAT - Inbound Prior Authorization File Validation		
Payer UAT - Inbound Recipient File Validation		

2. PROJECT MANAGEMENT OVERVIEW

2.1. ACTIVITIES BY PHASE

The following activities will be carried out by phase of the project. See highlighted for items specific to testing:

Table 2: Activities by Project Phase

Phase	Activities
Prior to Start	• Contracts Signed. • Teams introduced, and roles assigned. • Project management approach agreed. • Standard documentation review.
Requirements Gathering	• Kick off meeting, typically onsite at Tellus or client site. • Requirements completed for any product enhancement requests or non-standard integration. • Any product enhancement change orders presented and executed.

Design	• Tellus and Client BA's coordinate with their respective architects and technology teams to design solution per the given requirements.
Construction	• Tellus and Client technology teams write the software. • User outreach and training typically starts during development but may begin earlier or later depending up scheduling details. • Test plan written jointly by Tellus and Payer.
QA	• Tellus and Client quality teams each QA- and regression- test their respective software deliveries. Note: Tellus uses continuous integration (CI) build-deploy so that all software checked in is automatically deployed to QA. • Full Tellus-Client integration testing begins with QA. • The goal of QA is to deliver a production-ready software solution into the UAT environment.
UAT	• Client acceptance tests the complete integrated solution. • Client sign-off on production acceptance.
Production	• Release of the production solution into a production environment.

2.2. KEY DELIVERABLES BY PHASE

The following are key deliverables that Tellus will delivery by sprint/phase.

Table 3: Key Deliverables by Project Phase

Phase	Deliverables

Prior to Start	• Product Implementation Guide (This Document).
	• Standard Integration Specifications (online):
	  ○ Data Dictionary.
	  ○ Sample Messages (Flat File and XML).
	  ○ XML Schema.
	• Product Technical Specifications.
	• Product User Guide.
	• Draft schedule.

Throughout the Project	• Updated task list that includes:
	  ○ Task.
	  ○ Reporter.
	  ○ Assignee.
	  ○ Due Date.
	  ○ Next steps.
	• Updated listing of open issues/defects.
	• Updated delivery schedule/sprint schedule.

End of Requirements Gathering	• Change Orders for any billable work:
	  o Recital of requirements.
	  o Proposed solution.
	  o Costs.
	  o Timeline impacts.
	• Client Implementation Document (DRAFT):
	  o Integration Specifications for any non-standard integration.
	  o Listing of client-requested product enhancements (change orders).

End of Design	• Any design updates to change orders or the Client Implementation Document.
End of Construction	• Unit- and Integration-tested software deployment into quality assurance (QA) environment. • Any updates to change orders or the Client Implementation Document. • Test plan written jointly by Tellus and Payer.
End of QA	• QA and regression-tested solution deployed into UAT environment, ready for user acceptance testing (UAT). • Any updates to change orders or the Client Implementation Document.
End of UAT	• UAT-tested and accepted software solution ready for deployment into a production environment. • Any as-built updates to change orders or the Client Implementation Document (Final).
In Production	• Production software solution deployed into a production environment. • Ongoing training and outreach per Master Software and Services agreement. • Ongoing Tier-1 and/or Tier-2 user support per Master Software and Services agreement. • Ongoing B-2-B Operations Support per Master Software and Services agreement. • Ongoing hosting per Master Software and Services agreement.

2.3. ENVIRONMENTS

Tellus operates the following environments for our software development lifecycle (SDLC):

Development (DEV)

- Environment used by developers to write source code, configure databases, etc.
- Developers use NetBeans Integrated Development Environment (IDE)
- Source code managed using BitBucket Distributed version control system.
- DEV deployments are made back into the dev environment for unit and integration testing.

Quality Assurance (QA)

- Environment used by Tellus QA testers for quality assurance and regression testing.
- Take continuous integration builds as developers check software into Git.
- QA Mobile devices with iOS operating system take releases from TestFlight, an Apple App Store analogue used for testing purposes.
- QA Mobile devices with Android operating system receive Android application package (APK) releases buy internal email from Tellus Build-Deploy manager.
- Tellus and client begin full integration testing in QA, so client should be ready to integrate QA environments.
- The goal is to address all issues in QA, deploying only production-ready software to UAT.

User Acceptance Testing (UAT)

- Environment used by Tellus UAT testers for quality assurance, regression, and smoke testing at times.
- Environment used by client UAT testers for integration and acceptance testing.
- QA Mobile devices with iOS operating system take releases from TestFlight.
- QA Mobile devices with Android operating system receive APK releases buy internal email from Tellus Build-Deploy manager.
- Tellus and client continue full integration testing in UAT.
- All production-blocker defects must be addressed in QA before a production deployment.

Production (PROD)

- Reserved for only fully-tested production releases.

Demo (DEMO)

- Used for demonstration and training purposes only.
- Typically takes production releases only.
- Has a preconfigured suite of demo data that is automatically restored each night to allow for a "clean" demo/test environment each day.

The following diagram illustrates the Tellus infrastructural organization.

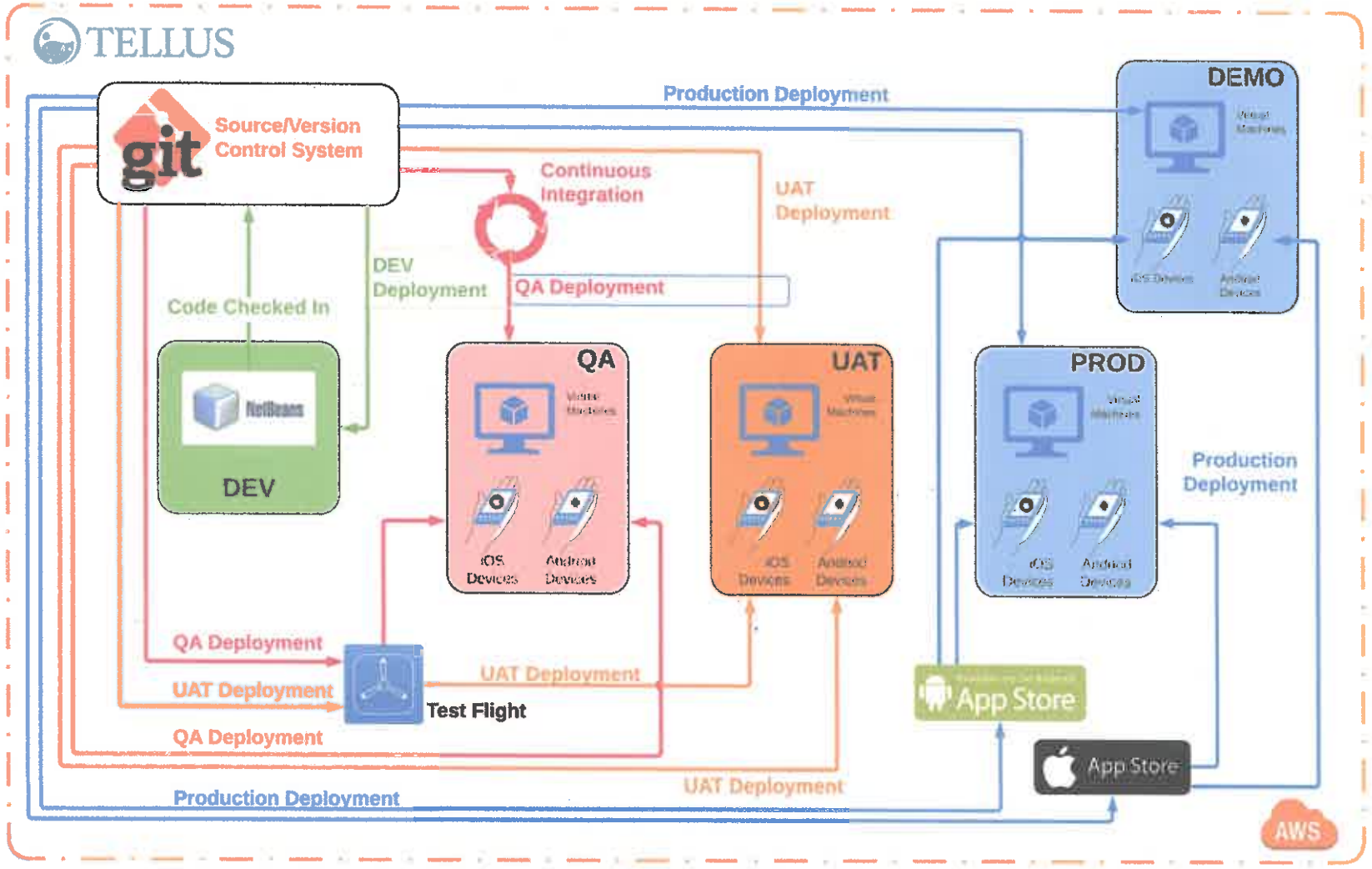


Figure 1: Tellus SDLC Infrastructure Diagram

2.4. PROJECT STAFFING

Tellus will staff each project according to requirements, but the general "package" is as follows:

Position	Description	Staffing
Senior Business Stakeholder	Senior manager who monitors the project, coordinates with client senior managers, and acts as an escalation point for any issues that may arise.	.1 Full Time Employee (FTE)
Solution Architect	Provides technical leadership with a focus on the vetting and design of any enhancement requests and any non-standard integration.	.1 FTE
Project Manager (PM)/Scrum Master (SM)	Provides project leadership, including: Single point of contact for the client, the management of task lists, the management of project schedule, management of project risks, the first line of resolution in any project issues, liaison between all other project participants.	.25 FTE
Business Analyst (BA)	The liaison between the business and technical teams. Focused on technical documentation including business requirements, use cases, functional specifications, data maps, etc.	1 FTE
Developers	A team of software developers of varying specialties.	1-2 FTE
Test Engineers	Tellus manages an ongoing quality assurance/quality control program that includes a full suite of new feature testing and regression testing on each release.	1-2 FTE

Payer staffing will depend on the details of the project, but if client-side software development is necessary, then the client team should roughly mirror the Tellus team. At minimum the client team will require a project manager to act as the single point of contact for Tellus, and to act as the coordinator of client-side staff.

3. TEST SCHEDULE AND GOVERNANCE

3.1. TEST PLANNING

Integrated testing will begin during the QA cycle, so planning for integration (FTP servers, test harnesses if necessary, etc.) must be completed during the development phase.

Notes on Preparation for Testing:

1. Please review the **Activities by Phase** and **Deliverables by Phase** sections above to understand the activities for QA vs. UAT testing.
2. Tellus will coordinate with you on test planning during the Development Phase.
3. See the **Environments** section above. Tellus will coordinate with you during the requirements phase to align Tellus-Payer environments.

Test Data Requirements:

1. Tellus does not allow for production data that contains PHI (Private Health Information), also known as personally identifiable information (PII) or non-public information (NPI) in any test environment. This means that you must be prepared to begin integration testing with scrubbed test data.
2. Plan to be ready to transmit test data via integrated channel (web services, FTP, etc.) by the beginning of the QA cycle.
3. Please plan for a daily test runs, or per the schedule that you agree with Tellus.
4. Data transmitted from Payer to Tellus is typically focused around recipient, prior authorization, and provider data sets. It is important that you create coordinated test data, so that the PA data aligns with the recipient and provider test data.
5. After Tellus receives the Payer test data, we will run test eVV visits and begin to generate claims data to return to your test systems. Please ensure that your recipient, prior authorization, and provider data sets contain sufficient variation to cover your test cases.

3.2. TEST SCHEDULE

Please refer to the project Gantt chart for QA and UAT test cycle dates.

3.3. REQUIRED TESTING RESOURCES

Testing will be performed by the Tellus and Payer Quality Assurance Test Teams. Test Engineers will be responsible for test case development, execution of tests, opening defect reports upon observance of nonconformance to documented requirements.

1. **Payer will be responsible for:**
   - 1.1. Generating test data for the recipient, provider, and PA feeds per this test plan and transmitting this data to Tellus.
   - 1.2. Receiving and processing 837P claims submission files from Tellus, including claims adjudication.
   - 1.3. Returning 999 and 835 (or agreed upon surrogate) files to Tellus for each 837P file transmitted by Tellus.
   - 1.4. Reporting any issues that may pertain to Tellus systems in a mutually agreed written softcopy format (typically a spreadsheet).
   - 1.5. Tracking and addressing any issues reported as pertaining to Payer systems using a mutually-agreed format (typically a spreadsheet).

2. **Tellus will be responsible for:**

2.1. Receiving and processing the recipient, provider, and PA feeds transmitted by Payer.

2.2. Generating and transmitting 837P claims submission files to Payer. This includes the scheduling, completion, and pre-adjudication of all test visits using the Tellus eVV platform.

2.3. Receiving and processing 999 and 835 (or agreed upon surrogate) files from Payer for each 837P file transmitted by Tellus.

2.4. Reporting any issues that may pertain to Payer systems in a mutually agreed written softcopy format (typically a spreadsheet).

2.5. Tracking and addressing any issues reported as pertaining to Tellus systems using a mutually-agreed format (typically a spreadsheet).

3.4. UAT ENTRANCE CRITERIA

Testing will begin at the direction of test management. The following criteria must be achieved prior to starting the UAT Testing Cycle.

- Requirements are defined and approved
- Completed testable code is available
- Test cases are developed and ready
- UAT test environment has been set-up and all other necessary resources are available
- Sufficient test data has been loaded into the test environment
- All known existing Top Priority defects have been resolved
- Smoke Testing has been executed and passed 100%

3.5. UAT TEST RELEASE CRITERIA

This section defines the targeted goals and conformance to exit UAT. Below are the UAT Exit Criteria:

Table 4: UAT Exit Criteria

REQUIREMENTS TRACEABILITY
All Planned Requirements have been Implemented & Delivered
All Requirements have been Tested
ACCEPTANCE TESTING

100% Test Case execution of all Acceptance Test Cases
100% Pass Rate of all Acceptance Test Cases

3.6. REQUIREMENTS TRACEABILITY CONFORMANCE

All Test Case to requirements traceability will be managed in Jira. Jira is an agile project management tool for creating and managing user stories, tasks, test cases, and defects.

4. TEST STRATEGY

4.1. FUNCTIONAL TEST OBJECTIVES & SCOPE

The purpose of this Test Plan is to define the testing objectives and overall testing approach for the Payer MCO v2.0 Integration with the Tellus Electronic Visit Verification (eVV) platform.

The approach of this testing effort is from an interface perspective, which is the operation of features and functions from external interfaces, which include the user interface and API interface. The primary focus will be black-box oriented; however, structural-testing techniques may be used to simulate environmental conditions and verify 'hidden' functions. Test types will include positive, negative, and error recovery.

The objectives for this testing effort are outlined below:

4.1.1. PRIOR AUTHORIZATION (PA) OBJECTIVES

4.1.1.1. Inbound Process New PA

Prerequisite: Provider and Recipient data used in test PA records already processed by Mirth and in the Payer database schema.

Objective: Validate Mirth "AAAA Processor Prior Authorization" channel processes the prior authorization file as a new prior authorization in the database.

Test Scope: The following scenarios are created from our Inbound Data Matching requirements for PA records. Scenarios are based on the logic for the following key data points in the PA record: PayerProviderId, RecipientMedicaidId, ServiceCode (including ServiceCodeMod1 and ServiceCodeMod2). If any of the key data points are not found in an existing database PA record, then a new PA record is created in the database. If all of the key data points match an existing database PA record, then the PayerAuthId and the AuthEffDate and AuthExpDate data range are evaluated. If the PayerAuthId does not match the existing PA record and AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. If the PayerAuthId does match the existing PA record and the AuthEffDate and AuthExpDate

date range does not overlap, then a new PA record is created in the database. After a PA batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the PA batch file, the number of PA records accepted, and the number of PA records rejected. Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the PA batch file with error codes and error descriptions for reconciliation by the client.

Notes: Tellus staff see the following link for inbound PA matching logic scenarios:

https://tellusolutions.atlassian.net/wiki/spaces/EVV/pages/488013832/Inbound+Data+Matching

4.1.1.2. Inbound Process Additional PA for Recipient - Same PA Number

Prerequisite: Provider and Recipient data used in test PA records already processed by Mirth and in the Payer database schema.

Objective: Validate Mirth "AAAA Processor Prior Authorization" channel processes the prior authorization file as an additional PA for same provider, recipient, service code, & PA number, but with a different non-overlapping date range.

Test Scope: The following scenarios are created from our Inbound Data Matching requirements for PA records. Scenarios are based on the logic for the following key data points in the PA record: PayerProviderId, RecipientMedicaidId, ServiceCode (including ServiceCodeMod1 and ServiceCodeMod2). If any of the key data points are not found in an existing database PA record, then a new PA record is created in the database. If all of the key data points match an existing database PA record, then the PayerAuthId and the AuthEffDate and AuthExpDate data range are evaluated. If the PayerAuthId does not match the existing PA record and AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. If the PayerAuthId does match the existing PA record and the AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. After a PA batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the PA batch file, the number of PA records accepted, and the number of PA records rejected. Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the PA batch file with error codes and error descriptions for reconciliation by the client.

Notes: Tellus staff see the following link for inbound PA matching logic scenarios:

https://tellusolutions.atlassian.net/wiki/spaces/EVV/pages/488013832/Inbound+Data+Matching

4.1.1.3. Inbound Process Additional PA for Recipient - Different PA Number

Prerequisite: Provider and Recipient data used in test PA records already processed by Mirth and in the Payer database schema.

Objective: Validate Mirth "AAAA Processor Prior Authorization" channel processes the prior authorization file as an additional PA for same provider, recipient, service code, with different PA number and a different non-overlapping date range.

Test Scope: The following scenarios are created from our Inbound Data Matching requirements for PA records. Scenarios are based on the logic for the following key data points in the PA record: PayerProviderId, RecipientMedicaidId, ServiceCode (including ServiceCodeMod1 and ServiceCodeMod2). If any of the key data points are not found in an existing database PA record, then a new PA record is created in the database. If all of the key data points match an existing database PA record, then the PayerAuthId and the AuthEffDate and AuthExpDate data range are evaluated. If the PayerAuthId does not match the existing PA record and AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. If the PayerAuthId does match the existing PA record and the AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. After a PA batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the PA batch file, the number of PA records accepted, and the number of PA records rejected. Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the PA batch file with error codes and error descriptions for reconciliation by the client.

Notes: Tellus staff see the following link for inbound PA matching logic scenarios:

https://tellusolutions.atlassian.net/wiki/spaces/EVV/pages/488013832/Inbound+Data+Matching

4.1.1.4. Adjust Existing PA

Prerequisite: Provider and Recipient data used in test PA records already processed by Mirth and in the Payer database schema.

Objective: Validate Mirth "AAAA Processor Prior Authorization" channel processes the prior authorization file as an additional PA for same provider, recipient, service code, & PA number the same or a different overlapping date range.

Test Scope: The following scenarios are created from our Inbound Data Matching requirements for PA records. Scenarios are based on the logic for the following key data points in the PA record: PayerProviderId, RecipientMedicaidId, ServiceCode (including ServiceCodeMod1 and ServiceCodeMod2). If any of the key data points are not found in an existing database PA record, then a new PA record is created in the database. If all of the key data points match an existing database PA record, then the PayerAuthId and the AuthEffDate and AuthExpDate data range are evaluated. If the PayerAuthId does not match the existing PA record and AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. If the PayerAuthId does match the existing PA record and the AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. After a PA batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the PA batch file, the number of PA records accepted,

and the number of PA records rejected. Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the PA batch file with error codes and error descriptions for reconciliation by the client.

Notes: Tellus staff see the following link for inbound PA matching logic scenarios:

https://tellusolutions.atlassian.net/wiki/spaces/EVV/pages/488013832/Inbound+Data+Matching

4.1.1.5. Error PA – Overlapping Dates

Prerequisite: Provider and Recipient data used in test PA records already processed by Mirth and in the Payer database schema.

Objective: Validate Mirth "AAAA Processor Prior Authorization" channel processes the prior authorization file as an additional PA for same provider, recipient, service code, but different PA number the same or a different overlapping date range. This is an error condition, PA's that meet these conditions are treated as duplicates.

Test Scope: The following scenarios are created from our Inbound Data Matching requirements for PA records. Scenarios are based on the logic for the following key data points in the PA record: PayerProviderId, RecipientMedicaidId, ServiceCode (including ServiceCodeMod1 and ServiceCodeMod2). If any of the key data points are not found in an existing database PA record, then a new PA record is created in the database. If all of the key data points match an existing database PA record, then the PayerAuthId and the AuthEffDate and AuthExpDate data range are evaluated. If the PayerAuthId does not match the existing PA record and AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. If the PayerAuthId does match the existing PA record and the AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. After a PA batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the PA batch file, the number of PA records accepted, and the number of PA records rejected. Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the PA batch file with error codes and error descriptions for reconciliation by the client.

Notes: Tellus staff see the following link for inbound PA matching logic scenarios:
https://tellusolutions.atlassian.net/wiki/spaces/EVV/pages/488013832/Inbound+Data+Matching

4.1.1.6. Rejected PA – Missing Required Fields

Prerequisite: Existing and non-existing provider and recipient records in the Tellus payer, provider, and recipient, database tables depending on the test case scenarios.

Objective: Validate Mirth "AAAA Processor Prior Authorization" channel processes the prior authorization file and rejects the record if the provider or recipient does not already exist in the payer, provider, or recipient database tables.

Test Scope: PA records are rejected in the following scenarios (non-existing means not in the Tellus payer database table and existing means is in the Tellus payer database table):

1. The PA record has a non-existing PayerProviderId and an existing RecipientMedicaidId
2. The PA record has an existing PayerProviderId and a non-existing RecipientMedicaidId
3. The PA record has a non-existing PayerProviderId and a non-existing RecipientMedicaidId

After a PA batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the PA batch file, the number of PA records accepted, and the number of PA records rejected. Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the PA batch file with error codes and error descriptions for reconciliation by the client.

4.1.2. PROVIDER MESSAGING TEXT OBJECTIVES

4.1.2.1. Create New Provider

Prerequisite: Provider does not already exist in Tellus payer database schema.

Objective: Validate Mirth "AAAA Processor Provider" channel processes the provider file as a new provider in the Tellus payer specific database schema.

Test Scope: A new provider record is created with data in the provider file if the provider does not already exist in Tellus payer database schema. Provider already existing or not existing is determined based on whether the PayerProviderId field value in the file is found or not found in the Tellus payer specific database schema. After a Provider batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the Provider batch file, the number of provider records accepted, the number of provider records accepted that were new records, the total number of provider records accepted that were updated records, the number of provider records rejected, and the current total of provider records in the payer specific provider database (including the records from the batch that generated the provider results email). Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the Provider batch file with error codes and error descriptions for reconciliation by the client.

4.1.2.2. Update Existing Provider

Prerequisite: Provider already exists in Tellus payer database schema.

4.1.3. RECIPIENT OBJECTIVES

4.1.3.1. Create New Recipient

Prerequisite: Recipient does not already exist in Tellus payer database schema.

Objective: Validate Mirth "AAAA Processor Recipient" channel processes the recipient file as a new recipient in the Tellus payer specific database schema.

Test Scope: A new recipient record is created with data in the recipient file if the recipient does not already exist in the Tellus payer database schema. Recipient already existing or not existing is determined based on whether the RecipientMedicaidId field value in the file is found or not found in the Tellus payer specific schema. After a Recipient batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the Recipient batch file, the number of recipient records accepted, the number of recipient records accepted that were new records, the total number of recipient records accepted that were updated records, the number of recipient records rejected, and the current total of recipient records in the payer specific recipient database (including the records from the batch that generated the recipient results email). Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the Recipient batch file with error codes and error descriptions for reconciliation by the client.

4.1.3.2. Update Existing Recipient

Prerequisite: Recipient does not already exist in Tellus payer database schema.

Objective: Validate Mirth "AAAA Processor Recipient" channel processes the recipient file with an update to an existing recipient record in the Tellus payer specific database schema.

Test Scope: A recipient record is updated with the data in the recipient file if the recipient already exists in the Tellus payer database schema. Recipient already existing or not existing is determined based on whether the RecipientMedicaidId field value in the file is found or not found in the Tellus payer specific schema. After a Recipient batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the Recipient batch file, the number of recipient records accepted, the number of recipient records accepted that were new records, the total number of recipient records accepted that were updated records, the number of recipient records rejected, and the current total of recipient records in the payer specific recipient database (including the records from the batch that generated the recipient results email). Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the Recipient batch file with error codes and error descriptions for reconciliation by the client.

4.1.3.3. Make Existing Recipient Ineligible

Prerequisite: Recipient already exists in Tellus payer database schema.

Objective: Validate Mirth "AAAA Processor Provider" channel processes the provider file with an update to an existing provider record in the Tellus payer specific database schema to make the recipient ineligible (scheduling disallowed, start visit disallowed) on Tellus eVV system.

Test Scope: A recipient record that contains a populated EligibilityEndDate that is <= current date, then the recipient should be disabled (scheduling disallowed, start visit disallowed) on the Tellus eVV platform. After a Recipient batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the Recipient batch file, the number of recipient records accepted, the number of recipient records accepted that were new records, the total number of recipient records accepted that were updated records, the number of recipient records rejected, and the current total of recipient records in the payer specific recipient database (including the records from the batch that generated the recipient results email). Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the Recipient batch file with error codes and error descriptions for reconciliation by the client.

4.1.4. CLAIMS MESSAGING TEST OBJECTIVES

4.1.4.1. Claims Submission via 837P (New Claim) Completed by Tellus

Prerequisite: Claim is in "Matched" status on the eVV Work List screen.

Objective: Validate that a Matched Claim can be submitted and generate an 837P Claims File.

Test Scope: A Provider Administrator can "release" a matched claim. Status is displayed as RELEASED. The "Released" claim is processed and an 837P Claims file is generated and sent to Payer. Once the claim is processed, the claim status will display as SUBMITTED.

4.1.4.2. Claims Submission via 837P (New Claim) processed by Payer

Prerequisite: Payer receives an 837P Claims File (New Claim).

Objective: Validate that an 837P Claims File (New Claim) is received, processed, accepted and an EDI 999 File (Implementation Acknowledgement) is generated and sent to Tellus eVV.

Test Scope: An 837P Claim File (New Claim) is received, processed, accepted and an EDI 999 File (Implementation Acknowledgement) responds with one of the following scenarios, 1) Accepted (no errors), 2) Accepted (with errors), or Rejected. If the 999 is Accepted with errors or Rejected, Payer's claims processing system responds with an EDI 835 (Health Care Claim Payment/Advice).

4.1.4.3. Claims Submission via 837P (Void Claim) Completed by Tellus.

Prerequisite: Claim is in "Paid" or "Denied" status on the eVV Work List screen.

Objective: Validate that a void claim transaction can be submitted and generate an 837P Claims File.

Test Scope: A Provider Administrator can "release" a void claim. Status is displayed as RELEASED. The "Released" claim is processed and an 837P Claims file is generated and sent to Payer. Once the claim is processed, the claim status will display as SUBMITTED.

4.1.4.4. Claims Submission via 837P (Void Claim) processed by Payer.

Prerequisite: Payer receives an 837P Claims File (Void Claim).

Objective: Validate that an 837P Claims File (Void Claim) is received, processed, accepted and an EDI 999 File (Implementation Acknowledgement) is generated and sent to Tellus eVV.

Test Scope: An 837P Claim File (Void Claim) is received, processed, accepted and an EDI 999 File (Implementation Acknowledgement) responds with one of the following scenarios, 1) Accepted (no errors), 2) Accepted (with errors), or Rejected. If the 999 is Accepted with errors or Rejected, Payer's claims processing system responds with an EDI 835 (Health Care Claim Payment/Advice).

4.1.4.5. Claims Submission via 837P (Adjusted Claim) Completed by Tellus.

Prerequisite: Claim is in "Paid" or "Denied" status on the eVV Work List screen.

Objective: Validate that an adjusted claim transaction can be submitted and generate an 837P Claims File.

Test Scope: A Provider Administrator can "release" an adjusted claim. Status is displayed as RELEASED. The "Released" claim is processed and an 837P Claims file is generated and sent to Payer. Once the claim is processed, the claim status will display as SUBMITTED.

4.1.4.6. Claims Submission via 837P (Adjusted Claim) processed by Payer.

Prerequisite: Payer receives an 837P Claims File (Adjusted Claim).

Objective: Validate that an 837P Claims File (Adjusted Claim) is received, processed, accepted and an EDI 999 File (Implementation Acknowledgement) is generated and sent to Tellus eVV.

Test Scope: An 837P Claim File (Adjusted Claim) is received, processed, accepted and an EDI 999 File (Implementation Acknowledgement) responds with one of the following scenarios, 1) Accepted (no errors), 2) Accepted (with errors), or Rejected. If the 999 is Accepted with errors or Rejected, Payer's claims processing system responds with an EDI 835 (Health Care Claim Payment/Advice).

4.1.4.7. Claims Submission via 837P (Denied Claim Resubmitted) Completed by Tellus.

Prerequisite: Claim is in "Denied" status on the eVV Work List screen.

Objective: Validate that a resubmit claim transaction can be submitted and generate an 837P Claims File.

Test Scope: A Provider Administrator can "release" a resubmit claim. Status is displayed as RELEASED. The "Released" claim is processed and an 837P Claims file is generated and sent to Payer. Once the claim is processed, the claim status will display as SUBMITTED.

4.1.4.8. Claims Submission via 837P (Denied Claim Resubmitted) processed by Payer.

Prerequisite: Payer receives an 837P Claims File (Resubmit Claim).

Objective: Validate that an 837P Claims File (Resubmit Claim) is received, processed, accepted and an EDI 999 File (Implementation Acknowledgement) is generated and sent to Tellus eVV.

Test Scope: An 837P Claim File (Resubmit Claim) is received, processed, accepted and an EDI 999 File (Implementation Acknowledgement) responds with one of the following scenarios, 1) Accepted (no errors), 2) Accepted (with errors), or Rejected. If the 999 is Accepted with errors or Rejected, Payer's claims processing system responds with an EDI 835 (Health Care Claim Payment/Advice).

4.1.4.9. 999 Generated by Payer

Prerequisite: An 837P has been sent to Payer.

Objective: Validate that Payer has responded with valid 999 file.

Test Scope: Payer generates and transmits the following test cases:

1. An EDI 999 File is transmitted to Tellus with each of the following scenarios:
   1.1. Accepted (no errors).
   1.2. Accepted (with errors).
   1.3. Rejected.

4.1.4.10. 277 Generated by Payer

Note: Tellus does not machine-process the 277 file, this file is stored for reference during troubleshooting.

Prerequisite: An 837P has been sent to Payer, Payer has responded with a 999 Accepted (with errors) or 999 Rejected file.

Objective: Validate that Payer has responded with valid 277 file.

Test Scope: Payer generates and transmits a 277 file.

2.2. PAID PARTIAL.

2.3. DENIED.

4.1.5. VISIT MANAGEMENT TEST OBJECTIVES

4.1.5.1. Overnight Visit

Prerequisite: A visit that span two days (e.g., an overnight stay through midnight) has been completed.

Objective: Validate the processing of a single visit for services performed by the Caregiver that begins on one day and finishes on another (spanning two days).

Test Scope:

1. Review and release the claim in Tellus eVV Provider Portal.
2. Validate that 837P claim file for this visit generated and transmitted as expected and with the correct number of units and dollar amount calculation for the claim.

4.1.5.2. Multiple Recipients on a Single Visit – No TT Modifier

Prerequisite: A scheduled and completed visit with more than one recipient on a single visit.

Objective: Validate the processing of a single visit for services performed by the Caregiver for two or more recipients.

Test Scope:

1. Review and release the claim in Tellus eVV Provider Portal.
2. Validate that 837P claim file for this visit generated and transmitted as expected and with the correct number of units and dollar amount calculation for the claim.

4.1.5.3. Multiple Recipients on a Single Visit – TT Modifier

Prerequisite: A scheduled and completed visit with HCPCS/service code with TT modifier (multiple recipients with discounts) and more than one recipient on a single visit.

Objective: Validate the processing of a single visit for services performed by the Caregiver for two or more recipients with TT modifier.

Test Scope:

1. Review and release the claim in Tellus eVV Provider Portal.
2. Validate that 837P claim file for this visit generated and transmitted as expected and with the correct number of units and dollar amount calculation for the claim, including discounts.

4.1.5.4. Multiple Service codes on a single visit

Prerequisite: A scheduled and completed visit with HCPCS/service code with no TT modifier (multiple recipients with discounts) and more than one recipient on a single visit.

Objective: Validate the processing of a single visit for services performed by the Caregiver for two or more recipients with no TT modifier.

Test Scope:

1. Review and release the claim in Tellus eVV Provider Portal.
2. Validate that 837P claim file for this visit generated and transmitted as expected and with the correct number of units and dollar amount calculation for the claim, with no discounts.

4.1.5.5. GPS Maximum Range Between Scheduled and Actual Start

Prerequisite: Visits are scheduled in the eVV system

Objective: Validate that visits are started and completed within specified allowable range from the scheduled location and ensuing claim is generated and transmitted by Tellus.

Test Scope: Scheduled visits will be completed in range increments including exact address (zero variance), a location slightly less than the maximum range (.5 mile), a location equal to the maximum range, and a location out of range followed by submission of a claim.

4.1.5.6. Completed Late Visit

Prerequisite: Visits are scheduled in the eVV system

Objective: Validate visits after the scheduled start and finish times.

Test Scope: Scheduled visits will be completed beyond of scheduled time with the following scenarios, 1) Started on-time, finished late, 2) Started late, finished on-time, and 3) Started late, finished late. Verify that all scheduled and actual times are gathered as expected, and that ensuing claim is generated and transmitted by Tellus.

5. DEFECT MANAGEMENT

The criteria used to determine whether each test case has passed or failed will be based on conformance to the User Stories, Use Cases, and/or requirements. Test cases that produce an actual output not consistent with the expected results will be considered as failed and a defect report will be opened in Jira. Jira will be used to track progress of each defect as they are resolved and retested until closed.

6. APPROVALS

Tellus and Payer have reviewed and approve this test plan. This plan will be used as the plan for the Quality Assurance (QA) and User Acceptance Testing (UAT) cycles of the above-mentioned project.

Tellus Signature:	Name:	Date:
_____	_____	_____
Client Signature:	Name:	Date:
_____	_____	_____

-- The Tellus Team Looks Forward to Working with You --

7. APPENDIX A - ACRONYMS & DEFINITION OF TERMS

7.1. ACRONYMS

Table 5: Acronyms Used in this Document

Term	Definition/Description
277	Healthcare Claim Acknowledgement (Error Details)
835	Healthcare Claim Acknowledgement (Claim Payment and Remittance Advice)
837P	Standard Formatted Electronic Healthcare Claim
999	Healthcare Claim Acknowledgement (File received)
ACA	Affordable Care Act
ACHA	The Agency for Healthcare Administration
API	Application Program Interface
AWS	Amazon Web Services
EVV	Electronic Visit Verification
FIT	Feature Integration Test
FTP	File Transfer Protocol
GA	General Availability
HIPAA	Health Insurance Portability and Accountability Act
HITRUST	The Health Information Trust Alliance
HHA	Home Health Aide
HHS	U.S. Department of Health and Human Services
HRSA	Health Resources and Services Administration
JIRA	Agile project management and defect tracking software application
JSON	Lightweight data-interchange format for data object transmission
MIRTH	Cross-platform HL7 interface engine enabling bi-directional messages
PA	Prior Authorization
ePHI	Electronic Protected Health Information
POS	Point of Service
PSD	Product Specification Document
SCM	Software Configuration Management
SVT	System Validation Test
TCS	Test Case Specification
TDS	Test Design Specification

7.2. DEFINITION OF TERMS

21st Century Cures Act	United States law enacted in December 2016 to accelerate the discovery, development, and delivery of 21st century cures, and for other purposes.
Acceptance Testing	Testing conducted to determine if the minimal requirements and/or specifications have been met and the product is ready for release.
Black-box Testing	Testing derived from a functional design specification without regard to the internal program structure and executed via end user or external interfaces.
Browser Compatibility Testing	Testing conducted to evaluate if an application or system works using different browsers.
Entrance Criteria	Metrics specifying the condition that must be met to begin testing at the next stage, phase, or level.
Exit Criteria	Metrics specifying the condition that must be met to promote a product or work unit to the next stage, phase, or level.
Exploratory Testing	Testing not derived specifically from a functional design specification but is executed via end user or external interfaces.
Functional Testing	Process of testing to verify that the functions of a system are present and operate as specified; testing from a block-box perspective. *Also known as Feature Testing*
Hardening Cycle	An additional sprint added for the purpose of executing Regression Testing, Bug Validation/Fixing, and specialty testing such as Security, Compliance, User Acceptance, prior to final release to production.
Production Environment	The environment where your system and services are made available to your customers.
Regression Testing	Testing that exercises a comprehensive set of test cases intended to verify that the system properly functions without degradation after changes have been applied.
Staging Environment	An environment that is a nearly exact replica of a production environment used for final updates and validation

	testing to assure the system is ready for Production. *Also known as UAT Environment.*
Stress Testing	Testing in which a system is subjected to unlikely or unrealistically harsh inputs (over loaded) or loaded with inadequate resources with the intention of identifying system limitations.
Structural Testing	Process of testing the consistency of a component's implementation with its design; testing from a white-box perspective
System Test	Testing to verify the product's integrated software, hardware, and documentation to the functional and operational requirements.
Visit	The act of performing a scheduled service by a trained caregiver.
White-box Testing	Testing derived from an internal design specification and/or the code and executed with knowledge of the internal program structure. *Also known as Clear-box Testing*

POL – 0EXE - 08
CHANGE CONTROL

Table of Contents

REVISION TABLE....2
PURPOSE....3
CONFIDENTIALITY, INTEGRITY AND AVAILABILITY....3
SCOPE....3
ACRONYMS AND DEFINITIONS....3
RESPONSIBILITIES....5
POLICY....5
Program Implementation....5
Change Management Board....5
Required Procedures....5
Upgrade Guidelines....7
No longer supported systems....7
Environmental Separation....8
Environments....8
Development (Dev)....8
Quality Assurance (QA)....9
Staging (STG)....10
User Acceptance Testing (UAT)....11
Production (Prod)....11
Operational Issue Prevention....12
REFERENCES....13

REVISION TABLE

Date	Description	Revised By	CCR #	Version
23 April 2018	Initial	Michael B. Morell, CISSP	A2TCS-26	.00
20 June 2018	Addition of Staging	Michael B. Morell, CISSP	A2TCS-26	.01
25 July 2018	Reviewed and approved	Michael B. Morell, CISSP	A2TCS-26	1.0
11 Aug 2018	Added C.I.A.	Michael B. Morell, CISSP	A2TCS-155	1.1
15 Aug 2018	Added Sub-Contractors	Michael B. Morell, CISSP	A2TCS-139	1.2
28 Sep 2018	Ready for Approval	Michael B. Morell, CISSP	A2TCS-26	1.3

PURPOSE

The purpose of this Policy is to give guidance on the Companies Change Control Program.

CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

This Policy shall demonstrate a clear commitment to maintaining and enforcing Confidentiality, Integrity, and Availability of Protected Health Information, Personally Identifiable Information and Non Public Personal Information.

SCOPE

Tellus has a commitment to maintaining and enforcing confidentiality, integrity, and availability of PHI.

The scope of this policy shall include the following areas:

1. Program Implementation
2. Change Control Board
3. Required Procedures
4. Environmental Separation

This policy applies to all Company employees, contractors, sub-contractors, consultants, temporary and other workers, and all third-party service personnel who access the Company network.

ACRONYMS AND DEFINITIONS

CCB – Change Control Board.

Company – This refers to Tellus, LLC Company as an entity.

DSO - Designated Security Officer. This person shall be designated by the CEO and identified as such in the organizational chart by the three (3) letter designation by their name.

Employee – unless otherwise stated, employee may mean any staff member of the company to include, full and part time employees, contractors, agents, and third parties acting on behalf of the company.

SCM – Software Configuration Management Team

RESPONSIBILITIES

1. The CEO is ultimately responsible for this policy and its approval.

2. The DSO is responsible for all changes, reviews, and updates to this policy. Reviews shall occur on a yearly basis.

3. The DSO is responsible for the creation of a Change Control Board.

4. The Change Management Board is responsible for the procedures required to enact changes and to give guidance on this Policy.

POLICY

Program Implementation

The Company shall institute a common change management program that shall be used across all departments.

Change Management Board

The DSO will create and oversee the Change Control Board (CCB). Each Department shall have a representative on the CCB.

Required Procedures

The CCB shall create procedures for the following items:

1. The manner of identifying and recording of significant changes.

2. The planning and testing of changes

3. Conduct the assessment of the potential impacts, including security impacts, of such changes.

    a. The system owner shall provide evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times.

b. This process shall include a risk assessment, analysis of the security and privacy impacts of changes, and specification of security controls needed. This process shall also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained.

4. Establish the formal approval of proposed changes.

5. Establish the communication of change details to all relevant persons

6. Ensure that as part of all change controls, that fallback procedures be defined and implemented, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.

7. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management

8. Establishes a process for identifying configuration items throughout the system development life cycle, and for managing the configuration of the configuration items.

9. Acceptance of new systems is clearly defined, agreed, documented and tested.

10. Perform unit, integration, system and regression testing/evaluation in accordance with organization-defined requirements for depth and coverage

11. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation

12. Implement a verifiable flaw remediation process.

    a. Correct flaws identified during security testing/evaluation.

    b. The Company shall require the developer of the information system, system component, or information system service to track security flaws and flaw resolution within the system, component, or service and report findings to Company-defined personnel or roles.

13. Ensure that a rollback strategy is in place before changes are implemented. Rollback procedures shall include backups of all relevant data that is being changed.

14. Rules for the migration of software from development to operational status shall be defined and documented by the Company hosting the affected application(s), including that development, test, and operational systems be separated (physically or virtually) to reduce the risks of unauthorized access or changes to the operational system.

Upgrade Guidelines

Any decision to upgrade to a new release shall take into account the business requirements for the change, and the security and privacy impacts of the release (e.g., the introduction of new security functionality or the number and severity of security problems affecting this version).

Prior to any changes to a Production environment, a current backup of all relevant data shall be conducted. Previous versions of application software shall be retained as a contingency measure. Old versions of software shall be archived, together with all required information and parameters, procedures, configuration details, and supporting software for as long as the data is retained in archive or as dictated by the company's data retention policy.

No longer supported systems

If systems or system components in production are no longer supported by the developer, vendor, or manufacturer, the Company must show evidence of a formal migration plan approved by management to replace the system or system components.

Environmental Separation

As part of the Change Control process, unique environments shall be maintained. The Change Control process will strive to create an environment that minimizes any testing on production systems. When testing must be performed, a test plan shall be developed that documents all changes to the system and the procedures for undoing any changes made to the system

Environments

Development (Dev)

The Dev environment is where all code is originated and initially tested. This environment access controls are controlled by the SCM team, while all code source is operated by the Dev team. The Development team Manager shall have final authority over what dev team members may access parts of source code or dev servers.

No Production data may be used or stored in Dev.

If covered, or otherwise sensitive, information must be used for testing purposes, all sensitive details and content shall be removed or modified beyond recognition (e.g., de-identified) before use.

The following requirements shall be applied to protect data, when used for testing purposes:

1. The access control procedures, which apply to operational application systems, shall also apply to test application systems.

2. There shall be formal management authorization for instances where operational information is copied to a non-production application system.

3. Operational information and test accounts shall be erased from a test application system immediately after the testing is complete.

Quality Assurance (QA)

The QA environment is the first environment that resembles Production, and where code may be tested, that will be simulating Production.

Environment Access shall be limited to those individuals that are required to perform QA activities. Code deployments to this environment shall require a change control but does not require CCB approval. In order to test instruction accuracy, code deployments into QA will be performed by both the SCM and Dev Team member.

No Production data may be stored or used in QA.

If covered, or otherwise sensitive, information must be used for testing purposes, all sensitive details and content shall be removed or modified beyond recognition (e.g., de-identified) before use.

The following requirements shall be applied to protect data, when used for testing purposes:

1. The access control procedures, which apply to operational application systems, shall also apply to test application systems.

2. There shall be formal management authorization for instances where operational information is copied to a non-production application system.

Operational information and test accounts shall be erased from a test application system immediately after the testing is complete.

Staging (STG)

The STG environment is where demos and training of the application are done. This environment is semi open, requiring username and passwords to enter, but is not restricted to solely customers and end users.

The STG environment shall closely resemble Production.

No Production data may be stored or used in STG.

Only test data may be used in STG. Any information entered into a STG system, must be fictitious.

Special note about user accounts

For applications such as demo sites, where the sales team are presenting the application to potential customers, it is preferred that unique usernames and password be generated for the customer.

The username and password for the demo portion of the environment may be generic while remaining unique to the customer. All such demo accounts will be deemed temporary and must be removed or deactivated within 48 hours of the presentation being concluded.

Training accounts shall be issued on a per user basis and shall be enabled for 30 days. After 30 days, a training account shall be automatically disabled.

User Acceptance Testing (UAT)

The UAT environment is where end users of the application can validate that the changes behave as expected. UAT environment access shall be restricted to only customers and end users that require access. When at all possible, the UAT environment shall not be made public.

The UAT environment shall closely resemble Production.

No Production data may be stored or used in UAT.

If covered, or otherwise sensitive, information must be used for testing purposes, all sensitive details and content shall be removed or modified beyond recognition (e.g., de-identified) before use.

The following requirements shall be applied to protect data, when used for testing purposes:

1. The access control procedures, which apply to operational application systems, shall also apply to test application systems.

2. There shall be formal management authorization for instances where operational information is copied to a non-production application system.

Operational information and test accounts shall be erased from a test application system immediately after the testing is complete.

Production (Prod)

Production environments consist of any architecture where its outage will have monetary loss or a loss of customer confidence. The following regions are considered to be Production:

1. Any Network Infrastructure where its outage would bring down any customer or internal systems.

2. Any Customer facing Server (web, database, application) that holds or processes production data.

Operational Issue Prevention

The level of separation between Dev, QA, UAT and Production environments shall be identified, with controls implemented to prevent operational issues.

Such controls shall include.

1. A review of all custom code preceding the release to production or to customers must be completed in order to identify any possible coding vulnerability.

2. Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices

3. Code reviews ensure code is developed according to secure coding guidelines.

4. Code-review results are reviewed and approved by management prior to release

5. Appropriate corrections to code are implemented prior to release to Production.

6. Develop, document, and maintain under configuration control, a current baseline configuration of the information system. The Company shall review and update the baseline configuration of the information system:

    a. at least once every six (6) months

    b. when required due to critical security patches, upgrades and emergency changes (e.g., unscheduled changes, system crashes, replacement of critical hardware components), major system changes/upgrades.

    c. as an integral part of information system component installations or upgrades.

    d. Supporting baseline configuration documentation reflects ongoing implementation of operational configuration baseline updates, either directly or by policy.

7. Any issues discovered in the in any environment must go thru all environmental level testing. For example. If an issue is discovered in UAT, it must be fixed in Dev and then tested in QA before deployment to UAT.

8. Prior to deploying to the Prod environment, all known bugs must be addressed in the lower environments.

9. Test data and accounts shall be removed completely before the application is placed into a production state.

10. All custom application accounts, user IDs, and passwords, shall be removed before applications go from development to production or are released to customer.

11. Development and operational software shall run on different systems with logical boundaries. Eg no development system can be on a production network/vlan.

12. Compilers, editors, and other development tools or system utilities shall not be accessible from QA, UAT or Production systems when not required.

13. The test system environments shall emulate the Production environment as closely as possible.

14. Unique Services accounts shall be created for each environment. No Dev, QA or UAT service accounts are allowed to be used in Production.

15. Users shall use different user profiles for operational and test systems, and menus shall display appropriate identification messages to reduce the risk of error.

REFERENCES

1. POL-0EXE-01-SecurityPolicy
2. POL-0MRK-01-CommunicationAndInformationDisclosure

POL – 0EXE - 02
RISK MANAGEMENT PROGRAM

Table of Contents

REVISION TABLE....3
PURPOSE....3
CONFIDENTIALITY, INTEGRITY AND AVAILABILITY....3
SCOPE....4
ACRONYMS AND DEFINITIONS....4
RESPONSIBILITIES....5
POLICY....5
Risk Management Program Areas....5
Phase 1: Risk Assessment....5
Phase 2: Business Continuity Planning....5
Phase 3: Disaster Recovery Planning....5
Risk Management Discovery Areas....6
Discovery Areas....6
Risk Criteria....8
Risk Analysis....10
Conducting a Risk Analysis....10
Vulnerability Assessments....11
Inclusion of risk areas....12
Permanent Risk Areas....12
Removal of risk areas....14
Defining Risk....15
Authorization of suspension of a Risk Analysis....15
Risk Report....15
Identified Risk Area Remediation....16
High Risk Systems....16
Disaster Recovery Sites....16
BCP and DR Concepts....17
BCP and DR Testing....18
Customer Specific BCP and DR planning....19
Service Providers....19
REFERENCES....20

REVISION TABLE

Date	Description	Revised By	CCR #	Version
23 April 2018	Initial	Michael B. Morell, CISSP	A2TCS-15	.00
11 Aug 2018	Added C.I.A.	Michael B. Morell, CISSP	A2TCS-155	.01
15 Aug 2018	Added Sub-Contractors	Michael B. Morell, CISSP	A2TCS-139	.02
28 Sep 2018	Approval	Michael B. Morell, CISSP	A2TCS-15	1.0

PURPOSE

This Company Risk Management Program, which includes Risk Assessment, Business Continuity Planning and Disaster Recovery Test Scripts, is intended to give define the role that Risk Management plays within the company.

The Risk Management Program provides the company with a framework in which to assess the various risks associated with doing business in its present form. The risk analysis framework is meant to serve as a guide to the assessor as to the procedures that are needed to be followed in order to complete an accurate assessment.

A formal Risk Analysis is meant to be prepared yearly and presented to Executive Management as well as the Board of Directors. The reports assessment is meant to guide the company to both resolving issues that it may or may not be aware of as well as serve as the foundation for the BCP/DR programs.

This program overview document is classified as Internal Use Only and may not be transmitted to third parties and clients with their solution specific plans.

For transmittal to third parties, please use POL-0EXE-03-RiskManagementProgramOverview

CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

This Policy shall demonstrate a clear commitment to maintaining and enforcing Confidentiality, Integrity, and Availability of Protected Health Information, Personally Identifiable Information and Non Public Personal Information.

SCOPE

Tellus has a commitment to maintaining and enforcing confidentiality, integrity, and availability of PHI.

The scope of the risk management program shall be based upon the Australian/New Zealand Standard "AS/NZS 4360:2004 Risk Management".

Utilizing the standard, this policy will define the following areas:

1. Risk Management Program Areas
2. Risk Management Discovery Areas
3. Risk Criteria
4. Risk Analysis
5. BCP and DR Concepts
6. Customer Specific BCP and DR planning
7. Service Providers

This policy applies to all Company employees, contractors, sub-contractors, consultants, temporary and other workers, and all third-party service personnel who access the Company network.

ACRONYMS AND DEFINITIONS

BCP - Business Continuity Planning. Business continuity planning involves assessing the risks to organizational processes and creating policies, plans, and procedures to minimize the impact those risks might have on the organization if they were to occur. BCP is used to maintain the continuous operation of a business in the event of an emergency situation. BCP is the foundation of the plan.

Company – This refers to Tellus, LLC company as an entity.

DSO - Designated Security Officer. This person shall be designated by the CEO and identified as such in the organizational chart by the three letter designation by their name.

Employee – unless otherwise stated, employee may mean any staff member of the company to include, full and part time employees, contractors, agents, and third parties acting on behalf of the company.

PII – Personally Identifiable Information

NPI – Non Public Information

PHI – Protected Health Information

RESPONSIBILITIES

1. The CEO is ultimately responsible for this policy and its approval.

2. The DSO is responsible for implementing the DR and BCP programs

3. Client Relationship Managers are responsible for ensuring that their customers have DR and BCP programs enacted for their solution.

POLICY

Risk Management Program Areas

The Risk Management Program consists of three areas: Risk Assessment, Business Continuity Planning and Disaster Recovery Test Scripts. All three areas have natural overlap.

Phase 1: Risk Assessment

In this phase, a Risk Assessment is performed against either company assets or a customer solution. Based on the information found in the Risk Assessment, a Business Continuity Plan is built.

Phase 2: Business Continuity Planning

In the BCP Phase, likely real world scenarios are applied to the various risk areas. "Likely" real world scenarios are preferred over "hypothetical" scenarios and garner a more realistic approach to developing a plan. The results that are found in this stage lay the foundation for the DR test scripts.

Phase 3: Disaster Recovery Planning

In this last phase, scripts are written that serve two purposes:

1. They can be used as a script to conduct controlled failure tests.

2. They can be used as a plan when an unexpected failure occurs.

The results of DR test scripts are typically, what are included with Audits and customer requests for BCP/DR plans.

Risk Management Discovery Areas

Utilizing RMP-0EXE-06-RiskAnalysis, pre-defined areas that require a risk analysis shall be maintained. The following is a general list and may be expanded on the risk analysis form without requiring update and approval to this policy. Removal of any items from this list will require an update and approval to this policy.

Discovery Areas

1. General
   This section of the Risk Analysis will define all of the stakeholders and establish the context of the objectives.

   a. Primary and Secondary Assessors shall be identified. The assessor is the individual responsible for conducting the Risk Assessment. The Assessor may be an internal resource or a 3rd party auditor.

   b. Stakeholders shall be identified for each division of the company. A stakeholder or 'responder', will be the individual(s) responsible for answering to the assessor, their areas of governance. A stakeholder may be assigned multiple areas of governance or may be secondary responders to a given risk area.

   c. Context Establishment is important in order to ensure that the objectives defined for the risk management process take into account the organizational and external environment.

      i. At the beginning of each new Risk Analysis primary objective will be defined. This will provide the overall direction for the risk analysis, as each year the objective may change.

      ii. In addition to a primary objective, a secondary objective may also be defined. This may be a complimentary objective to the primary.

      iii. The defining of any ancillary objectives shall also be included. Unlike Primary and Secondary objects, ancillary objectives do not have a direct impact on the overall direction, but are information that would help with the overall assessment.

2. Corporate Systems
   This section is used to define Corporate specific systems that can impact the overall company work flow. Items may be:
   a. Domain Controllers
   b. Mail Servers
   c. PBX systems
   d. File Servers
   e. Development Systems
   f. End users switches
   g. Internal Name Servers

3. Shared Infrastructure
   Shared Infrastructure is defined as items that are not expressly used for just company or client access. Items may be:

   a. Firewalls
   b. Load Balancers
   c. Database Servers
      i. Production
      ii. UAT
      iii. QA
   d. Web Servers
   e. FTP Servers
   f. External Name Servers

4. Staffing
   In the staffing section, define the critical positions required to maintain the core efficiency of each department.

5. Security
   Review the following areas:

   a. Information Security Program
   b. Third Party Agreements
   c. Change Management Procedures

6. Procedures and Best Practices
   A review of all key systems should be made as to their operating procedures and best practices that are applied.

7. Customer
   If the risk analysis is being generated for a customer, customer specific items would be identified and listed.

8. External Parties with Access to Sensitive Information
   If the risk analysis is being generated for a third party (vendor, business partner, etc.) with access to sensitive information, then third party-specific items would be identified and listed.

9. Service Providers
   If the risk analysis is being generated for a service provider that does not have access to sensitive information, then service provider-specific items would be identified and listed.

10. Overall Assessment
    In this portion of the Risk Analysis, each area will have risk ratings assigned to it. The higher the risk rating, the more resources will be needed to mitigate the risk.

Risk Criteria

Risk Criteria are items that are to be applied to each identified area or risk. These common items will be used to give an overall measurement of risk. Each risk area will be identified as having one of two main Risk Criteria applied to it; Business Continuity or Disaster Recovery.

Each Risk Area is required to have at least one of the two main criteria applied, but may have both if deemed appropriate.

At the beginning of each Risk Analysis cycle, the Risk Criteria will be reviewed. At a minimum, it shall contain the following:

a. Defining the architecture or process of the risk area.

b. Define the current requirements.

c. Establishing if the requirements have been met.

d. Establishing if the requirements can be met using the current architecture.

e. Defining the business impact of the risk area if it fails to operate normally.

f. Based upon the three risk criteria (c, d and e) an overall risk rating will be applied to the risk area.

g. Give an overall recommendation or assessment of the risk area.

Risk Analysis

Conducting a Risk Analysis

A risk analysis is to be conducted on a yearly basis, but is not to exceed more than 18 months between analyses. In addition, any significant change in the environment, or any change that may have a significant impact, as well as new products or services, must have a risk analysis performed.

All Risk Analysis will be part of the Companies change control procedures.

At the beginning of the Risk Analysis cycle, the DSO shall appoint a primary Assessor to conduct the yearly Risk Analysis. They (DSO) shall inform all department heads and executive management of the intent to begin the yearly analysis. The primary assessor may appoint a secondary assessor.

A process will be established to identify and assign a risk ranking to newly discovered security vulnerabilities. The risk ranking shall consider the CVSS score, classification of the vendor supplied patch, and/or the classification and criticality of the affected system.

The previous year RMP-0EXE-06-RiskAnalysisTemplate will serve as the foundation to conduct the current year analysis.

The assessor shall solicit responses from each identified stakeholder. Each stakeholder shall make themselves available to the assessor. In lieu of direct communication, email may be substituted as a communication method. The stakeholders however, are ultimately responsible for providing to the assessor information in a timely manner.

Assessor should have the knowledge of the following for each of their areas:

1. External environment factors that could exacerbate or moderate any or all of the levels of the risk components described in previous assessments.
2. The types of accounts offered by the Company.
3. The methods the Company provides to open and access its accounts.
4. Knowledge and experiences of incident histories and actual case impact scenarios on systems architectures.

During the analysis, the assessor may find items that are deemed either as continual low risk or items that have remained in high risk. In those scenarios the following may apply:

a. Items that have been identified in two consecutive years as having no/low risk, may be marked as no change.

b. Items that have been identified as high risk in two consecutive years, shall require the stakeholder of that system to submit a formal explanation as to why it has not been resolved; which shall be then attached to the final report.

Vulnerability Assessments

As part of the Risk Analysis, vulnerability assessments shall be commenced for the following areas and schedule

1. Internal vulnerability scan
   This scan consists of automated testing of all server systems. It shall be conducted on a monthly basis, have historical reports and will contain the following areas.

   a. Patch Levels
   b. Zero Day exploits
   c. Root Kits
   d. Misconfigurations that can lead to exploitation
   e. Information Leakage

2. Workstation Patch scans
   This scan consists of continuous automated monitoring of user workstations for patch level compliance.

3. Web Application Vulnerability Assessment
   This assessment shall be a formal yearly assessment performed by an accredited third party. All customer web applications that contain PHI/NPI/PII shall be required to have an independent assessment completed. The DSO shall engage an independent assessor, whom shall report their finding to the DSO. The DSO shall verify the report and engage any teams required to remedy any issues. The DSO shall provide Executive Management with a final report. The final report shall be included with the yearly risk analysis. The focus of the assessment shall be whether or not it is reasonable possible to obtain PHI/NPI/PII data from the web applications.

4. Enterprise Vulnerability Penetration Test
   This assessment shall be a formal penetration test performed every two years by an accredited, independent third party, with the intent to exploit the enterprise network.

   The assessment shall concentrate on the entire public footprint of the company. The Assessment shall include, at a minimum, the following areas.

   a. All internet facing sites and applications that can be discovered using standard information gathering techniques.

   b. Social engineering of end users.

Inclusion of risk areas

During the analysis, stakeholders may submit new risk areas to be included into the Risk Analysis, based on changes in procedure or architecture. It is understood by the stakeholder, that those items shall be carried over into the next year's analysis.

It is at the assessor's discretion to add those areas into RMP-0EXE-06-RiskAnalysis-Template, thus making those items non-susceptible to removal.

Permanent Risk Areas

Due to the sensitive nature, the following Risk Areas shall be a permanent part of all Risk Analysis, and may not be removed by any employee of the Company, to include Executive Management.

1. Ensuring the safety of personnel and the protection of information assets and organizational property.

2. Any system that houses NPI/PII/PHI must have a risk analysis performed. The methodology shall, at a minimum, address the following factors:

   a. The nature of the NPI/PII/PHI involved, including the types of identifiers involved and the likelihood of re-identification.

   b. The unauthorized person who used the NPI/PII/PHI or to whom the disclosure was made.

   c. Whether the NPI/PII/PHI was actually acquired or viewed.

   d. 4. the extent to which the risk to the NPI/PII/PHI has been mitigated

3. Capacity Planning

    a. The availability of adequate capacity and resources shall be planned, prepared, and managed to deliver the required system performance.

    b. Projections of future capacity requirements shall be made to mitigate the risk of system overload.

4. Backups

    a. Complete restoration procedures shall be defined and documented for each system.

    b. The Company ensures that backups, including remote and cloud-based backups, are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network.

    c. Regular testing of back-up media and restoration procedures shall be performed.

    d. If the back-up service is delivered by a third party, the service level agreement shall include the detailed protections to control confidentiality, integrity, and availability of the back-up information.

5. Secure Disposal Techniques. Validate that the Sanitization equipment and procedures for intended sanitization is being achieved.

6. Network Architecture Diagrams and security review.

7. Application Architecture Diagrams and security review.

8. Active Directory Group Policies

9. Central Patch management systems

10. Central Monitoring Systems

11. Antivirus Configuration Systems

12. Technical Vulnerability Management, to include internal and external vulnerability assessments.

13. The Company shall identify potential accessibility problems to alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

    The Company shall develop alternate processing site agreements that contain Priority-of-Service provisions in accordance with the organization's availability requirements, including recovery time objectives (RTOs).

    The alternate location shall be at a sufficient distance to escape any damage from a disaster at the main site.

    The type of configuration for the alternate site shall be defined by the risk assessment. Acceptable solutions include:

    a. cold sites - a facility with adequate space and infrastructure to support the system.

    b. warm sites - partially equipped office spaces that contain some or all of the system hardware, software, telecommunications and power sources

    c. Hot sites - office spaces configured with all of the necessary system hardware, supporting infrastructure and personnel

    d. mobile sites - self-contained, transportable shells custom-fitted with IT and telecommunications equipment necessary to meet the system requirements.

Removal of risk areas

During the course of the analysis, it may be found that risk areas either no longer exist or whose existence will not have a negative impact if they were to no longer exist.

Risk Areas that are identified as such shall require the following:

a. For areas that are part of RMP-0EXE-06-RiskAnalysis-Template, the stakeholder must submit in writing, a request to the assessor to have it removed. The assessor will make a recommendation to executive management as to its removal or continued inclusion. Executive management is solely responsible for the authorization of its removal.

b. For areas that are not part of RMP-0EXE-06-RiskAnalysis-Template, the stakeholder may informally request to the assessor that it may be removed. It is at the assessor's discretion to remove the item. All items that are disputed shall be given to executive management for resolution.

Defining Risk

Risks can be dealt with in one of four ways:

1. Avoidance - This approach eliminates the risk by avoidance of the activity which provides the risk. For example, the risk associated with utilization of wireless technologies can be mitigated by deciding not to use wireless technologies at all.

2. Reduction - Risk can be reduced by way of controls that can reduce the likelihood or impact of a risk. An example would be encryption of network traffic to minimize risks that threaten the confidentiality of data.

3. Transference - Risk can be reduced by shifting it to an outside entity. An example would be the purchase of insurance against fire damage.

4. Acceptance - Organizations can choose to accept risk by not selecting any of the aforementioned approaches. When acceptance is selected, management acceptance must be documented.

Authorization of suspension of a Risk Analysis

Any analysis that exceeds 18 months since the last will require a letter from Executive Management authorizing the suspension of the analysis and the reasoning.

The authorization of suspension is to be included in all yearly audits as additional documentation.

Risk Report

At the conclusion of the Risk Analysis, executive management shall be given a report that includes all risk areas. High and medium risk areas shall be given higher precedence in the report. Included in the report will be an overview of the enterprise security posture.

Identified Risk Area Remediation

While conducting a Risk Assessment, any failure items that have been identified, shall have timely action to remedy the failure item. Once a potential technical vulnerability has been identified, the Company shall identify the associated risks and the actions to be taken. Such action shall involve patching of vulnerable systems and/or applying other controls.

If a patch is available, change control procedures for the implementation of security patches and software modifications shall be followed. This shall include assessing the risks associated with installing the patch (i.e., the risks posed by the vulnerability should be compared with the risk of installing the patch). Patches shall be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated.

If no patch is available, is delayed, or not applied, other controls shall be applied including:

1. Documentation of impact.
2. Documented change approval by authorized parties.
3. Functionality testing to verify that the change does not adversely impact the security of the system.
4. Back-out procedures.
5. Turning off services or capabilities related to the vulnerability.
6. Adapting or adding access controls (e.g., firewalls) at network borders.
7. Increased monitoring to detect or prevent actual attacks.
8. Raising awareness of the vulnerability.

High Risk Systems

The technical vulnerability management process shall be evaluated on a quarterly basis in order to ensure its effectiveness and efficiency. Systems at high risk shall be addressed first.

Disaster Recovery Sites

Patches are installed in the production environment will also installed in the Companies disaster recovery environment in a timely manner.

BCP and DR Concepts

The Company, as a standard across all solutions, employs realistic risk analysis against all solutions so that a comprehensive plan can be formulated to protect against failures

The program is broken down into two areas

1. Business Continuity Planning (BCP)

   Business Continuity Planning, for the purposes of the Company, are built against scenarios. Scenarios are broken down into different risk groups and are based upon the discreet infrastructure identified during the Risk Analysis.

2. Disaster Recovery Planning (DR)

   Disaster Recovery Planning and test scripts, for the purposes of the Company, are built against the discreet infrastructure identified by both the Risk Analysis and BCP. This allows for the segmentation and testing of individual pieces on how they react to continuity risks, to give the greatest protection against failures.

The BCP/DR program includes several items:

1. Risk Analysis. This is where all components of a given solution are identified and issued a risk rating. Items with high risk ratings must have a BCP analysis done.

2. Business Continuity Planning. Based on the areas of Risk identified during the Risk Analysis, a scenario based plan will be written for each area. The scenario based plan will include instructions on what to do during a failure of that area.

3. DR Test Script. Based on the BCP, individual items are identified. Test scripts are developed to test each failure area. This is where explicit failure tests are conducted and the behavior recorded.

4. DR Yearly Test Matrix. The test matrix is where the items identified in the test plan or "script" are given a pre-determined testing scheduled such as; Annual, Bi-Annual, or Quarterly. Each test matrix is unique for the calendar year.

5. DR Test Log. This is where the discreet results of the test script are logged. Each log corresponds to a test date and may include items from the different schedule types.

6. DR Test Log Errors. This is where any failures of the test script are logged. Each log corresponds to a test date and may include items from the different schedule types. Any failure items will need to have a risk assessment performed recovery options adjusted and re-tested until a successful pass has been obtained.

BCP and DR Testing

A variety of techniques shall be used in order to provide assurance that the plan(s) will operate in real life including:

1. Table-top testing of various scenarios (discussing the business recovery arrangements using example interruptions)

2. Simulations (particularly for training people in their post-incident/crisis management roles)

3. Technical recovery testing (ensuring information systems can be restored effectively) including:

    a. system parameters are set to secure values
    b. security critical patches are reinstalled
    c. security configuration settings are reset
    d. system documentation and operating procedures are readily available
    e. application system software is reinstalled and configured with secure settings; and information from the most recent secure back-up(s) is loaded
    f. testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site)
    g. tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment)

4. Complete rehearsals (testing that the organization, personnel, equipment, facilities, and processes can cope with interruptions).

Customer Specific BCP and DR planning

Test scripts and DR planning documents are created specifically for a customer before their solution enters production. These documents cover "real" failure scenarios, which are Risk driven that have a realistic chance of occurring rather than an un-probable theoretical chance.

These documents are meant to be 'living' documents and can be revised as both sides see fit. The Company welcomes any input of "solution specific" testing scenarios, as long as those scenarios fit the guidelines of 'probable' rather than table top theory.

Service Providers

Service Providers of the Company shall be subject to the Risk Management Program.

Key areas that shall be tested are:

1. A review of service level agreements (SLAs) shall be conducted at least annually and compared against the monitoring records.

2. Service reports produced by the Service Provider shall be collected on an annual basis.

3. Audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to the service delivered shall be reviewed.

4. The Company shall monitor the network service features and service levels to detect abnormalities and violations. The Company shall periodically audit the network services to ensure that network service providers implement the required security features and meet the requirements agreed with management, including with new and existing regulations.

5. Verify that Service Providers use appropriate change management procedures for any changes to a third-party service or organizational system.

Third Partiers with Access to Sensitive Information

Important Note: Tellus does not provide third-parties with access to sensitive information as a policy. This section is included only in the event that a documented exception is approved.

Service Providers of the Company shall be subject to the Risk Management Program.

Key areas that shall be tested are:

1. A review of service level agreements (SLAs) shall be conducted at least annually and compared against the monitoring records.

2. Service reports produced by the Service Provider shall be collected on an annual basis.

3. Audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to the service delivered shall be reviewed.

4. The Company shall monitor the network service features and service levels to detect abnormalities and violations. The Company shall periodically audit the network services to ensure that network service providers implement the required security features and meet the requirements agreed with management, including with new and existing regulations.

5. Verify that Service Providers use appropriate change management procedures for any changes to a third-party service or organizational system.

REFERENCES

1. POL-0EXE-03-RiskManagementProgramOverview
2. RMP-0EXE-06-RiskAnalysis-Template

TELLUS

POL – 0FIN - 03
eVV Vendor Transition or Termination

(954) 719-0004
sales@4tellus.com
www.4tellus.com

© 2017-2019 Tellus, LLC

TABLE OF CONTENTS

1. PURPOSE 5
2. SCOPE 5
3. ACRONYMS AND DEFINITIONS 6
4. RESPONSIBILITIES 6
5. CONTACT INFORMATION 6
6. SOP 6

© 2017-2018 Tellus, LLC

800 Fairway Drive · Suite 360 · Deerfield Beach, FL 33441

STATEMENT OF CONFIDENTIALITY

This document contains confidential and proprietary information of Tellus, LLC ("Tellus") and is supplied to allow the recipient to make an evaluation of Tellus as a candidate for the delivery of software solutions and professional services. The recipient(s) of this document agree to inform present and future employees who receive or have access to this proposal of the confidential nature of this item and to instruct each employee not to disclose any information concerning this document to others without prior written consent from a dully authorized Tellus representative. The recipient further agrees to protect said confidential information as internal confidential information would be protected and not to disclose any information concerning this document to others without prior written consent from a dully authorized Tellus representative. The recipient of this document agrees not to duplicate or permit others to duplicate any material contained hereunder except for internal use.

© 2017-2018 Tellus, LLC

800 Fairway Drive · Suite 360 · Deerfield Beach, FL 33441

REVISION HISTORY

NAME	CCR #	REVISION DATE	VERSION	DESCRIPTION OF CHANGES
Chris Pernicano		9/29/2019	1.0	Initial Draft

© 2017-2018 Tellus, LLC

800 Fairway Drive · Suite 360 · Deerfield Beach, FL 33441

1. PURPOSE

Tellus operates as an Electronic Visit Verification (eVV) vendor in an environment that includes primary clients who may be managed care organizations (MCO's) or state Medicaid programs, secondary clients who are home care agencies or fiscal agents, and other eVV Vendors with the same type of clients.

The purpose of this document is to define Tellus policies and standard operating procedures (SOP) for the following three types of business event:

1. Tellus wins business to replace another eVV vendor as the eVV provider for a home care agency or similar. In this case the surrendering eVV vendor must share eVV-related data with Tellus to ensure an orderly transition.
2. Tellus loses business to be replaced by another eVV vendor as the eVV provider for a home care agency or similar. In this case Tellus must share eVV-related data with receiving eVV vendor to ensure an orderly transition.
3. Tellus' contract with an MCO or state Medicaid program ends and Tellus must share/return data to the primary client to ensure an orderly transition.

Important Note: This document does not address the legal agreements that must be put in place to allow for the sharing of protected health information (PHI) between business entities.

2. SCOPE

The scope of data to be transitioned is as follows:

1. Payer census data (names, identifying codes, etc.)
2. Payer prior authorization data.
3. Provider census data (names, identifying codes, etc.)
4. Recipient/Member census data (names, Medicaid ID, etc.)
5. Caregiver/Attendant census data (names, identifying codes, etc.)
6. Visit data for completed visits (all 21st century cures act data and supporting data).

Items that are beyond the scope of this document includes:

1. Visit scheduling information for future visits.
2. Claims submission data.
3. Ancillary documentation such as recipient care plans, etc.
4. Graphical data such as signature graphics.

3. ACRONYMS AND DEFINITIONS

1. **Governing Entity** – Typically a state Medicaid program or their representative, the organization that sets standards for Medicaid data interchange within a jurisdiction such as a state. In many cases the Governing Entity and the Receiving Entity may be the same.

2. **Surrendering Entity** – The eVV Vendor that is surrendering eVV data either to another eVV vendor or to a client such as a state Medicaid program or MCO.

3. **Receiving Entity** – The eVV Vendor or entity such as MCO or state Medicaid program that is receiving eVV data from a surrendering eVV vendor.

Note: Depending upon the situation, Tellus may play the role of either Surrendering Vendor or Receiving Entity.

4. RESPONSIBILITIES

1. Governing Entity:
   1.1. To coordinate with the vendors in the space to arrive at a standard for the sharing of eVV data that is within the above scope. The standard should at the least:
      1.1.1. Include full policy and procedure documentation.
      1.1.2. Include full technical specifications, including but not limited to:
         1.1.2.1. Data dictionaries.
         1.1.2.2. Collaboration diagrams or other documentation that describes entity relationships and cardinality.
         1.1.2.3. Sample files.
         1.1.2.4. Test harnesses.
      1.1.3. Tellus recommends that a format such as XML or JSON is used for this data interchange, to allow for the entire data set to be encapsulated in a single data file that can be downloaded or exported from the Surrendering Entity system and imported or uploaded into the receiving system.
   1.2. Provide the legal & communication framework for the data transfer described in this document:
      1.2.1. Legal requirements to initiate a transition.
      1.2.2. Document templates such as a standard form to initiate the transition.
2. Surrendering Entity:
   2.1. Make commercially reasonable effort to coordinate with the receiving vendor in good faith to provide the transition data in a timely fashion per the specifications provided by the Governing Entity.
3. Receiving Entity:
   3.1. Make commercially reasonable effort to coordinate with the surrendering vendor in good faith to receive and process the transition data in a timely fashion per the specifications provided by the Governing Entity.

5. CONTACT INFORMATION

Tellus:

txsupport@4tellus.com
833.894-3888

6. SOP

1. Preparation:
   1.1. Governing Entity provides specifications for data transition.
   1.2. Surrendering and Receiving entities design, implement, and test software to meet these specifications.
2. Data Transition:
   2.1. (Transition Date – 45 calendar days): Receiving Entity completes all necessary agreements and communicates the transition to the Surrendering Entity per the legal framework set out by the Governing Entity.

2.2. (Transition Date – 35 calendar days): Surrendering Entity acknowledges the request.
2.3. (Transition Date – 25 calendar days): Surrendering Entity provides draft copy of transition data file to receiving entity.
2.4. (Transition Date – 25-15 calendar days): Surrendering Entity and Receiving Entity coordinate to resolve any issues with the draft transition data file.
2.5. (Transition Date – 15-5 calendar days): Quiet time.
2.6. (Transition Date – 5 calendar days): Surrendering Entity transmits final draft copy of transition data file.
2.7. (Transition Date – 5-1 calendar days): Surrendering Entity and Receiving Entity coordinate to resolve any issues with the final draft transition data file.
2.8. (Transition Date – 1 calendar days): Surrendering Entity transmits production copy of transition data file.
2.9. (Transition Date):
    2.9.1. Receiving Entity makes their eVV system available to client beginning use of their platform (if applicable).
    2.9.2. Surrendering Entity disables access to any clients who are leaving the platform.
2.10. (Transition Date + 10 calendar days): Surrendering Entity certifies that surrendered data has been purged from their systems, with the exception of any data requires per data retention agreement.

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.

West Virginia Ethics Commission

Disclosure of Interested Parties to Contracts

(Required by *W. Va. Code* § 6D-1-2)

Name of Contracting Business Entity: 4Tellus LLC **Address:** 800 Fairway Dr, Suite 360 Deerfield Beach, FL 33441

Name of Authorized Agent: Joseph Schnur **Address:** 800 Fairway Dr, Ste 360. Deerfield Beach FL 33441

Contract Number: CRFP 0511 BMS2000000001 **Contract Description:** Electronic Visit Verification (EVV) RFP

Governmental agency awarding contract: West Virginia Department of Health and Human Resources Bureau for Medical Services

☐ **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.

   BRADLEY LEVINE

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: _____ Date Signed: January 27, 2020

Notary Verification

State of FLORIDA, County of BROWARD:

I, Joseph Schnur, 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 31st day of January, 2020.

_____
Notary Public's Signature

Notary Public State of Florida
Christine Gonzalez
My Commission GG 209481
Expires 08/17/2022

To be completed by State Agency:

Date Received by State Agency: _____

Date submitted to Ethics Commission: _____

Governmental agency submitting Disclosure: _____

Instructions for completion of Appendix 1 - Detailed Specifications

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.
2. Capability Assessment values are "Will Meet", Vendor agrees to specification or "Will Not Meet", Vendor declines to meet the specification.
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."
4. Using Tab 3 - Specifications & Responses, the Vendor should provide the Attachment, Section, and Page Number(s) where its detailed narrative response or acknowledgement for each specification resides.
5. Be advised that the Attachment column has been pre-populated with the location that the Department anticipates the narrative response to reside; however it is up to the Vendor to update the column accordingly if the Vendor should respond to a specification in a different location.
6. Hierarchy Level: The hierarchy level column defines relationships between parent and child specifications. DHHR refers to parent specifications as those that rely on the content of the related child specifications to fully define the scope of the requirement. DHHR refers to child specifications as those 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 (parent) 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. See the diagram below for an illustration of a hierarchy relationship:

-Hierarchy Level 1 Specification (parent)

-Hierarchy Level 2 Specification (child)

Tabs in this spreadsheet	
1. Worksheet Instructions	Contains instructions for completion of this RFP supplement.
2. Worksheet Information	Contains information about the contents of this workbook.
3. Specifications & Responses	Contains the specifications and all related data.
4. Code Values	Contains coded values for use in the specifications and response tab, and explanations as appropriate.

Columns on the specification Responses Tab

Section	Column	Description	Corresponding Code Values
Specifications	*Req ID #*	The unique ID of the specification.	N/A
	RTM ID (hidden)	The unique ID of the specification within the requirement traceability matrix. This is an internal reference field. Do not reference this field as part of the response process.	N/A
	Hierarchy Level	The hierarchy of the specification.	N/A
	Specification Text	The text of the specification.	N/A
Type	*N/A*	How the specification is categorized in the RFP.	N/A
Vendor Response Area	*Attachment*	Vendor is expected to provide a reference to the appropriate RFP attachment where more detailed information about the specification can be found. The expected attachment is identified for Vendor and the Department's convenience.	Attachment
	Section and Page Reference	Vendor is expected to provide a reference to its RFP response by Section and Page Number where more detailed information about the specification can be found.	N/A

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		
PG002	5140	2	Day	Program Management	Will Meet	Attachment 7 – Business Specifications Approach		
PG003	5141	2	Week	Program Management	Will Meet	Attachment 7 – Business Specifications Approach		
PG004	5142	2	Month	Program Management	Will Meet	Attachment 7 – Business Specifications Approach		
PG005	5143	2	Year	Program Management	Will Meet	Attachment 7 – Business Specifications Approach		
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		
PG007	4001	1	The solution should have the ability to round service delivery time.	Program Management	Will Meet	Attachment 7 – Business Specifications Approach		
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		
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		
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		
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		
PG012	4519	1	The solution should automatically generate all required correspondence to individuals.	Program Management	Will Meet	Attachment 7 – Business Specifications Approach		
PG013	4523	1	The Vendor should provide correspondence metric reports upon request by the Department.	Program Management	Will Meet	Attachment 7 – Business Specifications Approach		
PG014	4552	1	The solution should assist users in identifying which sections of forms should be filled in manually.	Program Management	Will Meet	Attachment 7 – Business Specifications Approach		
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		
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		
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		
PG018	4888	2	Member receiving services	Program Management	Will Meet	Attachment 7 – Business Specifications Approach		
PG019	4889	2	Direct care worker	Program Management	Will Meet	Attachment 7 – Business Specifications Approach		
PG020	4890	2	Provider	Program Management	Will Meet	Attachment 7 – Business Specifications Approach		
PG021	4891	2	Location of visit	Program Management	Will Meet	Attachment 7 – Business Specifications Approach		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		
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		
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		
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		
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		
PI006	5208	2	Payers	Program Integrity	Will Meet	Attachment 7 – Business Specifications Approach		
PI007	5209	2	Programs	Program Integrity	Will Meet	Attachment 7 – Business Specifications Approach		
PI008	5210	2	Provider Agency	Program Integrity	Will Meet	Attachment 7 – Business Specifications Approach		
PI009	5211	2	Direct care workers	Program Integrity	Will Meet	Attachment 7 – Business Specifications Approach		
PI010	5212	2	Members	Program Integrity	Will Meet	Attachment 7 – Business Specifications Approach		
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		
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	I. Visit Verification	
/V002	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	I. Visit Verification	
V003	5075	2	Individual receiving services	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	I. Visit Verification	
V004	5076	2	Direct care worker	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	I. Visit Verification	
V005	5077	2	Billing provider agency	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	I. Visit Verification	
V006	5079	2	Location of visit	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	I. Visit Verification	
V007	5080	2	Date of visit	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	I. Visit Verification	
V008	5081	2	Visit start time	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	I. Visit Verification	

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
VV009	5082	2	Visit finish time	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	I. Visit Verification	
VV010	5083	2	Missed visits	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	I. Visit Verification	
VV011	5084	2	Late visits	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	I. Visit Verification	
VV012	5085	2	Services delivered, including billing code and modifiers	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	I. Visit Verification	
VV013	5086	2	Independent verification by individual receiving services	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	I. Visit Verification	
VV014	5087	2	Payer	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	I. Visit Verification	
VV015	5088	2	Manual or electronic verification	Visit Verification	Will Meet	Attachment 7 – Business Specifications Approach	I. Visit Verification	
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	I. Visit Verification	
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	I. Visit Verification	
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	I. Visit Verification	
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	I. Visit Verification	
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	I. Visit Verification	
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	I. Visit Verification	
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	I. Visit Verification	
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	I. Visit Verification	
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	I. Visit Verification	
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	I. Visit Verification	
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	I. Visit Verification	
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	I. Visit Verification	
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	I. Visit Verification	

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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	I. Visit Verification	
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	I. Visit Verification	
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	I. Visit Verification	
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	I. Visit Verification	
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	I. Visit Verification	
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		
DD002	5116	2	Data classes	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD003	5117	2	Attributes	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD004	5118	2	Relationships	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD005	5119	2	Standards	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD006	5121	2	Other data elements identified by the Department	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
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		
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		
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		
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 Meet	Attachment 8 - Technical Specifications Approach		
DD014	5138	1	The solution should have the ability to store member communications.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		
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		
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		
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		
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		
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		
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 Meet	Attachment 8 - Technical Specifications Approach		
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		
DD023	4912	2	Member name	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD024	4913	2	Billing provider	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD025	4914	2	Name	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD026	4915	2	Date	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD027	4916	2	Time of service delivery	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
DD031	4475	1	The solution should generate all forms and notices as necessary.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		
DD033	4470	1	The solution should allow printing of blank and completed documents including, but not limited to:	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD034	4935	2	All forms	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD035	4936	2	All system-generated correspondence	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD036	5104	2	Reports	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD037	4481	1	The solution should generate and supply forms in the following methods, including, but not limited to:	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD038	4482	2	Email	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD039	4483	2	Download from Portal	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD040	4484	2	Postal Mail, upon request by the Department	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
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 Meet	Attachment 8 - Technical Specifications Approach		
DD042	4478	1	The solution should allow updates to form templates as directed by the Change Management Plan.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
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 Meet	Attachment 8 - Technical Specifications Approach		
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 Meet	Attachment 8 - Technical Specifications Approach		
DD045	4487	1	The solution should automatically populate information on notices or forms being issued.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD046	4490	1	The solution should generate batch forms.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD047	4493	1	The solution should save delivered forms to the user's account.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
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 Meet	Attachment 8 - Technical Specifications Approach		
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 Meet	Attachment 8 - Technical Specifications Approach		
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 Meet	Attachment 8 - Technical Specifications Approach		
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 Meet	Attachment 8 - Technical Specifications Approach		
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 Meet	Attachment 8 - Technical Specifications Approach		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
DD053	4544	1	The solution should generate correspondences using pre-defined templates	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD054	4546	1	The solution should include automatic system-generated correspondence with output capabilities including, but not limited to:	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD055	4960	2	Email	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD056	4962	2	Post to user portal account	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD057	4963	2	Queue for printing	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD058	4547	1	The solution should be able to schedule distribution of correspondence.	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
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		
DD063	4973	2	Excel	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD064	4974	2	Word	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD065	4975	2	Hyper Text Markup Language (HTML)	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD066	4982	2	Comma-Separated Value (CSV)	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD067	4984	2	Portable Document Format (PDF)	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
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		
DD072	4817	2	Multi-tasking and multiple window capability, including split screens	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
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		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		
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		
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		
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		
DD078	4863	2	Pull-down menus and window tabs	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD079	4864	2	Scalable, true-type screen and printing fonts	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD080	4865	2	Uppercase and lowercase alphabetic characters	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
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		
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 Meet	Attachment 8 - Technical Specifications Approach		
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		
DD087	4918	2	Create flags	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD088	4919	2	Send alerts	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
DD089	4920	2	Integration of alerts into the workflow	Data Sources, Delivery, & Display	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
DQ001	3993	1	The solution should provide a method to identify the following:	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
DQ002	5049	2	National Provider Identifier (NPI)	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
DQ003	5050	2	Healthcare Common Procedure Coding System (HCPCS)	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
DQ005	5136	2	State-specific codes defined by the Department	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
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		

Specifications					Vendor Response			
Req ID.#	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
DQ007	5039	2	Definition of data elements	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
DQ008	5040	2	Data file formatting	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
DQ009	5041	2	Data exchange frequency	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
DQ010	5042	2	Thresholds for data quality and acceptance	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
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		
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		
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		
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		
DQ018	4569	1	The solution should report on both duplicated and unduplicated record counts.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
DQ019	4588	1	The solution should use consistent data schemes and version control.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
DQ023	4587	1	The solution should identify and use consistent report fields	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
DQ024	4586	1	The solution should display a consistent format on all reports.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
DQ026	4990	2	Source system	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
DQ027	4991	2	Data content	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
DQ028	4992	2	Purpose	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
DQ029	4993	2	Frequency	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
DQ031	5095	2	Manual edits	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
DQ032	5096	2	Error corrections	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
DQ033	5097	2	Additions to the interface records	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
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		
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		
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 Meet	Attachment 8 - Technical Specifications Approach		
DQ040	4492	1	The solution should have the ability to identify which fields in forms are required and which are optional.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
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 Meet	Attachment 8 - Technical Specifications Approach		
DQ042	4545	1	The solution should provide automatic default file naming convention for saved correspondence as agreed upon with the Department.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
DQ043	4553	1	The solution should categorize and classify types of correspondence as agreed upon with the Department.	Data Quality	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
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		

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		
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		
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		
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		
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		
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		
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		
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		
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		
IN007	5090	2	Communication events (email, document upload, form submissions, or phone)	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN008	5091	2	System-generated events	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN009	5092	2	User-triggered events	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN010	5093	2	Exception-processing events	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
IN012	4529	1	The solution should have the ability to facilitate mass email notifications.	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
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 Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		
IN018	4401	2	Telephone	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN019	4402	2	Member portal	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN020	4403	2	Email	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN021	4404	2	Mail	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
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		
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		
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		
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		
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		
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		
IN031	4922	2	Creation of tickets	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN032	4923	2	Editing existing tickets	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN033	4924	2	Sorting of call center ticket information	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN034	4925	2	Filtering of call center tickets or electronic records	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
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		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
IN036	4417	2	The caller	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN037	4418	2	The question(s) and/or issue(s)	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN038	4419	2	The Vendor staff responding to the ticket	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN039	4420	2	The date(s)	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN040	4421	2	The time(s)	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN041	4422	2	The status (opened or closed)	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN042	5217	2	Problem resolution	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
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		
IN047	5031	2	Persons with Limited English Proficiency (LEP)	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN048	5032	2	Persons with vision disabilities	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN049	5033	2	Persons with hearing disabilities	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN050	5034	2	Persons with speech disabilities	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
IN053	5191	2	Microsoft Edge	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN054	5192	2	Apple Safari	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN055	5193	2	Google Chrome	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN056	5194	2	Mozilla Firefox	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
IN057	5195	2	Microsoft Internet Explorer	Hardware and Infrastructure	Will Meet	Attachment 8 - Technical Specifications Approach		
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 Meet	Attachment 8 - Technical Specifications Approach		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
SM009	3977	1	The solution should use role-based access for data and system functionality.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		
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		
SM012	5043	2	User name	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM013	5044	2	Date of access	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM014	5045	2	Time of access	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
SM016	5047	2	Name of computer system used to access confidential personal information (CPI)	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM017	5048	2	Query/Transaction used	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM018	4082	1	The solution should provide users role-based access to reporting functionality.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM019	5218	1	The solution should allow correspondence to be viewed based on role based access.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM020	4564	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		
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		
SM022	5052	2	Unique identifiers (IDs)	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
SM024	5054	2	Profile or group access assignments	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
SM027	5055	2	Blocking specific window or screen access	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM028	5056	2	Blocking specific report views or analytics	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM029	5057	2	Restrict data elements	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		

Specifications					Vendor Response			
Req ID #	RFM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
SM030	5058	2	Restrict viewing of specific members	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
SM034	4240	1	The solution should have the ability to restrict concurrent logons.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
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		
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		
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		
SM041	5061	2	Monitoring and reporting of events on an ongoing basis	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
SM043	5157	2	Non-compliant and required security and privacy controls	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM044	5158	2	Applied mitigations	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM045	5159	2	Plan to correct deficiencies	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		

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		
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		
SM050	4591	2	Who requested the information	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM051	4592	2	Date of request	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM052	4593	2	Time of request	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM053	4594	2	What data the report included	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM054	4595	2	Report storage upon completion	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
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 Meet	Attachment 8 - Technical Specifications Approach		
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		
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 Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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 Meet	Attachment 8 - Technical Specifications Approach		
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 Meet	Attachment 8 - Technical Specifications Approach		
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 Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
SM066	4488	1	The solution should allow users to override and change pre-populated information in forms, when appropriate.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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 Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
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		
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		
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		
SM074	5016	2	Page level	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM075	5017	2	Field level	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM076	5018	2	Data element level	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
SM078	4848	2	Instructions on how to use the secure site	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM079	4849	2	Site map	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM080	4850	2	Contact information	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
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 Meet	Attachment 8 - Technical Specifications Approach		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		
SM083	5021	2	Provider number	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM084	5022	2	Prior authorization number	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM085	5023	2	Medicaid ID number	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM086	5024	2	Date of service	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM087	5025	2	Claim number	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM088	4755	1	The solution should allow a system administrator to reset user passwords.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM089	4756	1	The solution should allow users to change their passwords on demand.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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 Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
SM095	4241	1	The solution should allow self-service password resets.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
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 Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
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		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		Attachment 8 - Technical Specifications Approach		
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		
SM103	4750	2	Preventive Controls: Controls designed to prevent errors and unauthorized events from occurring	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
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		
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		
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		
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		
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 Meet	Attachment 8 - Technical Specifications Approach		
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 Meet	Attachment 8 - Technical Specifications Approach		
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		
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		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
SM115	4266	2	Invalid login attempts	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM116	4267	2	Transaction activities	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM117	4268	2	Track adds, changes, and deletes of individual member visit verification data	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM118	4269	2	Password changes	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM119	4270	2	Security question and/or Key creation	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM120	4271	2	Updates to security questions	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM121	4272	2	User navigation history	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
SM124	4276	2	User Identification	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM125	4277	2	Machine/Internet Protocol Address Identification	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM126	4278	2	Time and Date of Action	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM127	4279	2	Actions Performed	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
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		
SM132	4247	1	The solution should support member-delegated authority including, but not limited to:	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM133	5161	2	Assistors	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
SM134	5162	2	Authorized representatives	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		Attachment 8 - Technical Specifications Approach		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
SM148	4310	2	Maintaining compatibility with Department software and systems.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
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		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		
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		
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		
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		
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		
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		
SM156	4328	1	The solution should have the ability to support non-disclosure of information.	Security Management	Will Meet	Attachment 8 - Technical Specifications Approach		
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		
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		
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		
PM002	5036	2	Rule deletion	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM003	5037	2	Rule modification	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM004	5038	2	Addition of new rules	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM005	5146	2	Business edits	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM006	5147	2	Others as defined by the Department	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
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		
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		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		
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		
PM024	5198	2	Applicable test cases	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM025	5199	2	Expected test results	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM026	5200	2	Others as defined by the Department	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
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		
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		
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		
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		
PM031	5201	2	Metrics on the number of tests completed	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM032	5202	2	Number of deferred or canceled tests	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM033	5203	2	Results of the tests executed	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM034	5204	2	Defects identified by severity level	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM035	5205	2	Corrective actions taken	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM036	5206	2	Others as defined by the Department	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
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		
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		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
PM051	5245	2	Unit testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM052	5247	2	Iterative functional testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM053	5248	2	System integration testing (SIT)	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM054	5249	2	Interface testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM055	5250	2	Regression testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM056	5251	2	End-to-end testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM057	5252	2	Security testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM058	5253	2	Performance testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM059	5254	2	Usability/Accessibility testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM060	5255	2	Browser testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM061	5256	2	User acceptance testing (UAT)	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM062	5257	2	Data conversion testing	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM063	5258	2	Operational readiness testing (ORT)	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM064	5259	2	Other testing as identified by the Department and/or Vendor	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
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		
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		
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		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
PM068	5263	2	Deployment of new solution components	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM069	5264	2	Integration of each solution component into the primary solution	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM070	5265	2	Every migration of new build versions to each test environment	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM071	5266	2	Solution fixes	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM072	5267	2	Solution patches	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM073	5268	2	Solution releases	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM074	5269	2	Others as defined by the Department	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
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		
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		
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		
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		
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		
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		
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		
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		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		
PM084	5280	2	Internal users	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM085	5281	2	External users	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM086	5283	2	Users with limited computer skills	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM087	5284	2	New user registration	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM088	5286	2	Users with disabilities	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM089	5287	2	Others as defined by the Department	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
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		
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		
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		
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		
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		
PM095	4969	2	Correct the report	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM096	4970	2	Verify the report	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM097	4971	2	Distribute or re-distribute the report	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		

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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
PM108	5232	2	Design documentation	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM109	5233	2	Code modules	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM110	5234	2	Test conditions	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM111	5235	2	Test scenarios	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM112	5236	2	Test cases	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM113	5237	2	Certification criteria	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
PM114	5238	2	Medicaid Information Technology Architecture (MITA) business areas and processes	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM115	5239	2	Medicaid Information Technology Architecture (MITA) Standards and Conditions	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
PM116	5240	2	Others as defined by the Department	Project Management	Will Meet	Attachment 9 - Implementation Specifications Approach		
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		
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		
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		
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		
TN002	5176	2	Members or Legal Representative	Training	Will Meet	Attachment 9 - Implementation Specifications Approach		
TN003	5177	2	Direct Care Workers	Training	Will Meet	Attachment 9 - Implementation Specifications Approach		
TN004	5178	2	Provider Agencies	Training	Will Meet	Attachment 9 - Implementation Specifications Approach		
TN005	5197	2	The Department	Training	Will Meet	Attachment 9 - Implementation Specifications Approach		
TN006	5179	2	Other as defined by the Department	Training	Will Meet	Attachment 9 - Implementation Specifications Approach		
TN007	3974	1	The Vendor should provide training at the time of registration.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach		
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		
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		
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		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		
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		
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		
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		
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		
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		
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		
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		
TN019	4168	1	The Vendor should provide a user manual to all users.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach		
TN020	4169	1	The user manual should be subject to Department approval.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach		
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		
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		
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		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		
TN025	5290	2	Security reminders (at login or screen access)	Training	Will Meet	Attachment 9 - Implementation Specifications Approach		
TN026	5291	2	Training reminders	Training	Will Meet	Attachment 9 - Implementation Specifications Approach		
TN027	5292	2	Online training capabilities	Training	Will Meet	Attachment 9 - Implementation Specifications Approach		
TN028	5293	2	Training tracking	Training	Will Meet	Attachment 9 - Implementation Specifications Approach		
TN029	5294	2	Others as defined by the Department.	Training	Will Meet	Attachment 9 - Implementation Specifications Approach		
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		
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		
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		
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		
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		
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		
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		
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		
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		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		
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		
OP002	4716	2	The estimated and actual hours allocated to each change request	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP003	4717	2	Specific personnel assigned to each change request	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP004	4718	2	Scheduled completion date for each change request	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
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		
OP006	4720	2	Any change to current operational costs	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
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		
OP008	5008	2	Others as defined by the Department	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
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 Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
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		
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		
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		
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		
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		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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		
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		
OP017	5131	2	No authorization	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP018	5132	2	Expired authorization	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP019	5133	2	Reasons that prevented claims from filing	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP020	5134	2	Edits made to claims	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP021	5135	2	Others as defined by the Department	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
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		
OP023	5100	2	Browser-based	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP024	5101	2	Portable Document Format (PDF)	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP025	5102	2	Excel	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP026	5103	2	Comma-Separated Value (CSV)	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP027	5172	2	Others as defined by the Department	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP028	4522	1	The solution should track metrics for each type of correspondence generated in the solution.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
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		
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 Meet	Attachment 10 - Maintenance and Operations Specifications Approach		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
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 Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
OP042	4928	2	Hours of operation	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP043	4929	2	Options for leaving messages after hours	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
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		
OP045	4931	2	Recording of informational messages as defined by the Department	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
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		
OP047	5108	2	Average speed of answer	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP048	5109	2	Interface processing time	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP049	5110	2	Request time for report generation	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP050	5111	2	Others as defined by the Department	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
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		
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		
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		
OP054	4939	2	Others as defined by the Department	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
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		
OP056	4940	2	Hardware	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP057	4941	2	Environment	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP058	4942	2	Network specifications	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		

Specifications					Vendor Response			
Req ID #	RTM ID	Hierarchy Level	Specification Text	Subject Matter Area	Capability Assessment	Attachment	Section	Page #
OP059	5106	2	Others as defined by the Department	Operations				
OP060	4661	1	The solution should provide real-time solution performance data.	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
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		
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 Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
OP063	4740	1	The solution should allow the Department's administrator to view, filter, sort, and search the error log(s).	Operations	Will Meet	Attachment 10 - Maintenance and Operations Specifications Approach		
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		
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		
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		
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		

Response Template: Description
Attachment 2: Cost Sheet
Attachment 3: Vendor Qualifications and Experience
Attachment 4: Project Organization and Staffing Approach
Attachment 5: Initial Work Plan
Attachment 6: Mandatory Requirements
Attachment 7: Business Specifications Approach
Attachment 8: Technical Specifications Approach
Attachment 9: Implementation Specifications Approach
Attachment 10: Maintenance and Operations Specifications Approach

Capability Assessment
Will Meet
Will Not Meet

Instructions for Completion of Attachment 6 - Mandatory Requirements

1. Using *Tab 3 - Mandatory Req & Responses*, the Vendor must provide the ***Attachment***, ***Section***, and ***Page Number(s)*** where its detailed narrative response or acknowledgement for each mandatory requirement resides.
2. The Vendor must ensure that each mandatory requirement is addressed.
3. Be advised that the ***Attachment*** column has been pre-populated with the location that the Department anticipates the narrative response to reside; however it is up to the Vendor to update the column accordingly if the Vendor should respond to a mandatory requirement in a different location.
4. Failure to affirmatively reply to any mandatory requirement will result in rejection of the Vendor's proposal.
5. ***Hierarchy Level***: The hierarchy level column defines relationships between parent and child mandatory requirements. DHHR refers to parent requirements as those that rely on the content of the related child to fully define the scope of the requirement. DHHR refers to child requirements as those that rely on additional context provided by a higher-level requirement (parent) to fully define the scope of the requirement. A hierarchy value of 1 denotes the highest-level (parent) requirement. Any greater hierarchy value denotes a child requirement. For example a hierarchy level 2 is a child to the nearest prior hierarchy level 1. See the diagram below for an illustration of a hierarchy relationship:

-Hierarchy Level 1 Mandatory Requirement
-Hierarchy Level 2 Mandatory Requirement

Tabs in this spreadsheet	
1. Worksheet Instructions	Contains instructions for completion of this RFP supplement.
2. Worksheet Information	Contains information about the contents of this workbook.
3. Mandatory Req Responses	Contains the mandatory requirements and all related data.
4. Code Values	Contains coded values for use in the mandatory requirements tab, and explanations as appropriate.

Columns on the Specification Responses Tab

Section	Column	Description	Corresponding Code Values
Mandatory Requirements	*Req ID #*	The unique ID of the mandatory requirement.	N/A
	RTM ID (hidden)	The unique ID of the mandatory requirement within the requirement traceability matrix. This is an internal reference field. Do not reference this field as part of the response process.	N/A
	Hierarchy Level	The hierarchy of the mandatory requirement.	N/A
	Specification Text	The text of the mandatory requirement.	N/A
Type	*N/A*	How the mandatory requirement is categorized in the RFP.	N/A
Vendor Response Area	*Attachment*	Vendor is expected to provide a reference to the appropriate RFP attachment where more detailed information about the requirement can be found. The expected attachment is identified for Vendor and the Department's convenience.	Attachment
	Section and Page Reference	Vendor is expected to provide a reference to its RFP response by Section and Page Number where more detailed information about the mandatory requirement can be found.	N/A

Mandatory Requirements						
Req ID #	Hierarchy Level	Requirement Text	Type	Attachment	Section	Page #
MR001	1	All provided services must comply with the Department rules.	Program Management	Attachment 6 - Mandatory Requirements	Program Management	60
MR002	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	Project Management	60
MR003	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	Hardware and Infrastructure	61
MR004	1	The solution must securely capture and electronically verify:	Visit Verification	Attachment 6 - Mandatory Requirements	Visit Verification	62
MR005	2	The identity of the member receiving services	Visit Verification	Attachment 6 - Mandatory Requirements	Visit Verification	62
MR006	2	The identity of the direct care worker making the visit	Visit Verification	Attachment 6 - Mandatory Requirements	Visit Verification	62
MR007	2	The identity of the provider agency	Visit Verification	Attachment 6 - Mandatory Requirements	Visit Verification	62
MR008	2	The date the visit begins and ends	Visit Verification	Attachment 6 - Mandatory Requirements	Visit Verification	62
MR009	2	The time the visit begins and ends	Visit Verification	Attachment 6 - Mandatory Requirements	Visit Verification	62
MR010	2	The location of the visit	Visit Verification	Attachment 6 - Mandatory Requirements	Visit Verification	62
MR011	2	The services being delivered	Visit Verification	Attachment 6 - Mandatory Requirements	Visit Verification	63
MR012	2	The waiver program or plan name	Visit Verification	Attachment 6 - Mandatory Requirements	Visit Verification	63
MR013	1	The solution must uniquely identify each user.	Security Management	Attachment 6 - Mandatory Requirements	Security Management	63
MR014	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	Data Sources, Delivery, and Display	64
MR015	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	Project Management	66
MR016	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	Security Management	66
MR017	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	Security Management	66
MR018	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	Security Management	67

Mandatory Requirements						
Req ID #	Hierarchy Level	Requirement Text	Type	Attachment	Section	Page #
MR019	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	Security Management	67
MR020	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	Security Management	67
MR021	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	Security Management	68
MR022	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	CMS Certification	69
MR023	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	CMS Certification	69
MR024	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	CMS Certification	72

Vendor's should not edit this worksheet.

Attachments
Response Template
Attachment 2 - Cost Sheet
Attachment 3 - Vendor Qualifications and Experience
Attachment 4 - Project Organization and Staffing Approach
Attachment 5 - Initial Work Plan
Attachment 6 - Mandatory Requirements
Attachment 7 - Business Specifications Approach
Attachment 8 - Technical Specifications Approach
Attachment 9 - Implementation Specifications Approach
Attachment 10 - Maintenance and Operations Specifications Approach

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: 4TEHUS LLC

Authorized Signature: _____ Date: 3/9/2020

State of FLORIDA

County of BROWARD, to-wit:

Taken, subscribed, and sworn to before me this 11th day of MARCH, 2020.

My Commission expires August 17th, 2020.

AFFIX SEAL HERE

Notary Public State of Florida
Christine Gonzalez
My Commission GG 208461
Expires 08/17/2022

NOTARY PUBLIC _____

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.

4Tellus LLC

(Company)

Joseph Schnur Joseph Schnur, CCO

(Authorized Signature) (Representative Name, Title)

Joseph Schnur, CCO

(Printed Name and Title of Authorized Representative)

January 24, 2020

(Date)

Phone: 941-228-2491 Fax: N/A

(Phone Number) (Fax Number)

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand 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.

4Tellus LLC

Company

Joseph Schnur

Authorized Signature

January 24, 2020

Date

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

SOLICITATION NUMBER: CRFP 0511 BMS2000000001
Addendum Number: 1

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[ ] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[ ] Attachment of vendor questions and responses

[X] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[ ] Other

Description of Modification to Solicitation:

To provide the pre-bid meeting sign-in sheets.

No other changes.

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

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)

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

4TELIVS LLC
Company

Authorized Signature

3/9/2020
Date

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

SOLICITATION NUMBER: CRFP BMS2000000001
Addendum Number: 2

The purpose of this addendum is to modify the solicitation identified as CRFP BMS2000000001 ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[ ] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[ ] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[X] Other

Additional Documentation:

1. To change the buyer and contact information on the CRFP.

   Brittany Ingraham, Senior Buyer, will now be the assigned buyer to the CRFP.
   Email: Brittany.E.Ingraham@wv.gov
   Phone number: 304-558-0067

2. Responses to vendor questions will be issued under separate addendum.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP 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)

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

4TELIVS LLC
Company

Authorized Signature

3/9/2020
Date

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

SOLICITATION NUMBER: CRFP 0511 BMS2000000001
Addendum Number: 3

The purpose of this addendum is to modify the solicitation identified as CRFP 0511 BMS2000000001 ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[X] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[ ] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[ ] Other

Additional Documentation: This purpose of this addendum is to:

1. Modify the bid opening date as follows:

   Bid opening WAS 01/27/2020 at 1:30 PM ET
   Bid opening IS NOW 02/14/2020 at 1:30 PM ET

Responses to vendor questions will be issued under separate addendum.

No other changes.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

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

4TELIVI LLC
Company

Authorized Signature

3/9/2020
Date

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

SOLICITATION NUMBER: CRFP 0511 BMS2000000001
Addendum Number: 4

The purpose of this addendum is to modify the solicitation identified as CRFP 0511 BMS2000000001 ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[X] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[ ] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[ ] Other

Additional Documentation: This purpose of this addendum is to:

1. Modify the bid opening date as follows:

   Bid opening WAS 02/14/2020 at 1:30 PM ET
   Bid opening IS NOW 02/28/2020 at 1:30 PM ET

Responses to vendor questions will be issued under separate addendum.

No other changes.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

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

ATELIVS LLC
Company

Authorized Signature

3/9/2020
Date

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

SOLICITATION NUMBER: CRFP 0511 BMS2000000001
Addendum Number: 5

The purpose of this addendum is to modify the solicitation identified as CRFP 0511 BMS2000000001 ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[X] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[ ] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[ ] Other

Additional Documentation: The purpose of this addendum is to:

1. Modify the bid opening date as follows:

   Bid opening WAS 02/28/2020 at 1:30 PM ET
   Bid opening IS NOW 03/12/2020 at 1:30 PM ET

Responses to vendor questions will be issued under separate addendum.

No other changes.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

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	[ ]	Addendum No. 6
[X]	Addendum No. 2	[ ]	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.

ATCIIVS LLC
Company

Authorized Signature

3/9/2020
Date

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

SOLICITATION NUMBER: CRFP 0511 BMS2000000001
Addendum Number: 6

The purpose of this addendum is to modify the solicitation identified as CRFP 0511 BMS2000000001 ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[ ] Modify bid opening date and time

[X] Modify specifications of product or service being sought

[X] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[X] Other

Additional Documentation: The purpose of this addendum is to:

1. Modify the specifications per the attached Change Log.
2. Provide vendor questions and agency responses per the attached.
3. Provide cost tables per the attached (attached as **Addendum #6 - EVV_RFP_Cost_Sheet_Tables**).
4. Provide 'Disclosure of Interested Parties to Contracts' Form per the attached.

No other changes.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

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	[ ]	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.

4TELLVS LLC
Company

Authorized Signature

3/9/2020
Date

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

SOLICITATION NUMBER: CRFP 0511 BMS2000000001
Addendum Number: 7

The purpose of this addendum is to modify the solicitation identified as CRFP 0511 BMS2000000001 ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[ ] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[X] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[ ] Other

Additional Documentation: The purpose of this addendum is to:

1. Provide Agency response to additional Vendor question.

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

No other changes.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

CRFP 0511 BMS2000000001
Addendum No.07
Electronic Visit Verification(EVV)

Vendor Question:

We have a question about the included Cost Sheet ("Addendum #6 - EVV_RFP_Cost_Sheet_Tables.xlsx").

Table 15 states to enter the monthly Recurring Deliverable Cost for each deliverable however on Table 13 is only pulls those costs over for once (i.e. one month of recurring deliverables), and it seems like it should factor it by 6 for the 6 months of implementation. Should the vendor enter the monthly cost per deliverable in table 15 and then the Agency will factor it by 6 months on table 13, or should the vendor enter the total costs for 6 months of the deliverables in Table 15?

Agency Response:

Vendors should include the total amount of each recurring deliverable in Table 15. The total amounts included in Table 15 will be equally divided and paid to the vendor monthly based upon their proposed implementation schedule, which is not to exceed 6 months. The total value from Table 15, which is used in Table 13 (cell D5) represents the total of all recurring payments to be made for these monthly deliverables.

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.

4TELLUS LLC
Company

Authorized Signature

3/9/2020
Date

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

environment employing loosely coupled services. Real-time rendered service data is available for claims pre-adjudication and 837 submission to MMIS on the day services are completed. Payer adjudication data can be imported to EVV and made available to providers as soon as the payer transmits the information to Tellus. Tellus can accept standard 835 or proprietary data formats.

2. **MITA Condition:** Tellus will assist the State in documenting "As-Is" and "To-Be" environments of business, information and technical capabilities demonstrating an increasing MITA maturity level, complying with MITA 3.0. Tellus will also strive to identify and recommend opportunities to leverage the reuse of health care technologies within the State and among other states.
3. **Industry Standards Condition:** Tellus EVV is fully compliant with the following standards: a. Health Insurance Portability Act of 1996 (HIPAA) b. Health Information Technology for Economic and Clinical Health Act (HITECH) c. National Institute of Standards and Technology (NIST) Special Publication (SP) 800 d. Section 508 of the Rehabilitation Act, Americans with Disabilities Act (ADA) e. Federal Civil Rights Laws f. Section 1104 of the Affordable Care Act g. Section 1561 of the Affordable Care Act h. 45 CFR 164.316 and Administrative Rule 37.85.414
4. **Leverage Condition:** Tellus supports the open/hybrid EVV model and publishes standard open Application Program Interfaces (APIs) promoting interoperability across the Medicaid ecosystem by integrating with care management applications, third-party EVV vendors and MMIS.
5. **Business Rules Condition:** Tellus is passionate about understanding the perspectives of all EVV constituents. Our communications, outreach, training and customer support initiatives strive to promote a community of reliability, trust and respect. Our EVV solution supports accurate claims processing processes and procedures.
6. **Reporting Condition:** Tellus EVV collects and evaluates all the data necessary to evaluate the operation and performance of the EVV program to monitor and improve operations, transparency and accountability. AWS CloudWatch is used to monitor network traffic, bandwidth usage and bottlenecks that impede performance. Monitoring and auto-scaling systems provide the information required to diagnose system performance issues, errors and backlogs. Monitoring includes, but is not limited to, CPU, memory utilization, network and disk utilization. For the database server, we also monitor read/write latency, number of sessions and session performance. Our engineers get immediate notifications about all system issues. If these cannot be resolved immediately, notifications will be forwarded to the State and/or Providers as required based on service level agreements.

7. **Interoperability Condition:** Tellus uses Mirth Connect, an open source, cross-platform, bi-directional health care integration engine providing maximum flexibility to integrate with health information exchanges, public health agencies, human service programs and other community organizations as required.

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.

As a rule, our EVV application is updated on a quarterly basis with release notes shared with clients in advance to make them aware of enhancements and provide access to training materials if necessary. We will share these artifacts with the WDH no less than seven (7) business days prior to the release. If required due to changes in Federally mandated or National Standards compliance requirements (including, but not limited to, CMS, HIPAA, MITA) or technical issues, the applications may be updated off cycle. All changes will be monitored through the documented change control process and communicated to constituents in a timely manner.

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.

All changes will be monitored through the documented change control process and communicated to constituents in a timely manner, including sign off when required.

PM011	4199	1	The solution should have the ability to allow the modification of edits per the Change Management Plan.

Tellus EVV is a COTS application configurable to meet your specific requirements thanks to our powerful business rules engine. Our methodology favors configuration over customization to accelerate implementation time, streamline testing and simplify change management.

The initial configuration is recorded in the CMDB (Configuration Management Database), provided through the Drools Business Rules Management System, which is an integral part of the solution. The configuration is therefore automatically logged and regularly maintained throughout the project lifecycle. Changes to the initial configuration are requested by the State and subsequently implemented and recorded in the integrated CMDB as they occur.

Tellus EVV is a SaaS-based application built from the ground up to provide maximum flexibility with minimal effort. Configuration settings, variable parameters and business rules that are separate from our code base provide the ability to deploy a highly flexible and adaptable solution for any environment very quickly.

At the heart of the system's flexibility and adaptability is our Rules Engine. Tellus EVV makes use of the RedHat Drools Rules Engine. The solution is comprised of a core Business Rules Engine (BRE), a web authoring and rules management application (Drools Workbench) and an Eclipse IDE plugin for core development. Key features are as follows:

- Drools is a Declarative Rules Engine.
- The Drools Inference Engine uses Rete algorithm for pattern matching.
- Engine supports Forward (iterate) & Backward (goal seek) chaining.
- Business rules version control is managed with the rest of our source code using the Git source control system. Rules rollback uses the same mechanism as software rollbacks.
- The Drools engine provides full debugging capabilities, including support for code step-through with break points, and the ability to see which rules have fired. Eclipse IDE includes a plugin that visualizes the RETE tree.
- Drools Flow offers a workflow design functionality in the form of blocks. The user specifies exactly which rules are executed in which order under which conditions.

Business rules are generally defined by payer. However, they can be created at any level, using the following hierarchy:

- Jurisdiction (State)
- Payer
- Plan
- Program

- Provider
- Caregiver
- Recipient

This classification system enables DHHR to configure the EVV application at the program level. Program rules, services, policies and procedures and reimbursement rates can be defined at the program/provider level. Business rules can also be written based on these categories as well as at the field level. Because our business rules engine is a module independent of the software code base, rules can be changed during the term of the contract without the use of development resources, providing maximum flexibility.

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.

The Tellus EVV platform supports a manual visit verification process that is adaptable to program requirements throughout the contract period as directed by the Change Management Plan. The form of visit verification is captured on each visit record so if a visit is manually verified, it will be designated as "manual". Reporting and data analytics can help DHHR monitor and evaluate manually verified services.

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.

Tellus EVV boasts a robust reporting platform that supports pre-defined periodic reporting as well as ad hoc custom reporting. Standard reports and recipients of reports can be changed easily over the life of the contract as define in the approved Change Management Plan.

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.

Tellus provides complete documentation for our EVV system, which is updated across the life of the project, and includes Administrative System Documentation accompanied by both User Guides and PowerPoint training materials in writing, as well as both live and recorded webinar training sessions and video "snippets" for commonly asked questions. This material encompasses complete Administrative System Functionality and reporting capabilities.

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.

Standard training guides including system documentation, user guides, FAQs and training materials will be published online so that the most current documents are always available. User documents are published in both English and Spanish. We will verify accuracy of all translations. User documents are continually updated as features and functions are modified and introduced into the software. We will work with you in developing innovative approaches to deliver the training content that works for your constituents

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.

Tellus EVV is flexible and adaptable to the different business processes for each of the State's programs, including waivers and services. The solution will be configured for all programs requested during the business requirements phase, to include unique business rules for waiver programs if requested.

Business rules are generally defined by payer. However, they can be created at any level, using the following hierarchy:

- Jurisdiction (State)
- Payer
- Plan
- Program
- Provider
- Caregiver
- Recipient

This classification system enables the State of West Virginia to configure the EVV application at the program level. Program rules, services, policies and procedures and reimbursement rates can be defined at the program/provider level. Business rules can also be written based on these categories as well as at the field level. Because our business rules engine is a module independent of the software code base, rules can be changed during the term of the contract without the use of development resources, providing maximum flexibility.

User-based permissions, combined with flexible rules, allow the ability to customize user privileges by program. That means a provider can be granted the right to enter service tasks on one program by personnel type and not have that same access for another program.

Service task lists can vary and be customized based on program needs and rules. A configurable option is to allow direct caregivers to enter notes and/or alerts using their mobile device to effectively and efficiently communicate recipient status to provider administrators and/or case managers.

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.

System, portal and application updates will be released on an ongoing and as needed basis. Releases will maintain functionality, security and integrity of data. Releases that include new features and functionality may introduce additional configuration options for existing clients. Features and functions for upcoming releases will be communicated in advance of the release and existing clients will be educated about the options available as a result of the enhancements or modifications. They can adopt those changes by changing applicable business intelligence rules and configuration settings

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.

Any changes to the software processing workflow will be managed through the standard Tellus Change Management Process. See Addendum D, Change Management.

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.

The project management plan, as well as the procedures documentation, will outline an effective change control method for the review, revision, and approval of planning documents, testing processes, and other project deliverables. We recommend a change control board (CCB) be created to provide feedback on identified changes, to review and approve modifications. The CCB should be formed early in the project and shall include DHHR and Vendor stakeholders.

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.

See attached Addendum D, Change Management.

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.

Risks will be documented in a Risk Management Plan created as part of the overall project management plan. and as such will follow PMBOK© guidelines. The Risk Management Plan will be supplemented by a risk register that includes both impact and probability ratings, prioritizations, responses, and contingency plans to address each of the identified risks. The register will be managed by the Project

Manager and will continue to change as the project progresses. Risk identification will be an activity that will continue through the completion of the contract.

See Addendum E, Risk Management

PM022	4116	1	The Vendor should coordinate all testing activities as agreed upon by the Department.

After configuration or coding, the testing team verifies the deliverables of the implementation phase against requirements using our Requirements Traceability Matrix (RTM). The testing team follows the Software Testing Lifecycle (STLC) which is similar to the development cycle adopted by the development team.

All development activities, including testing, are driven by user requirements, system specs, the Interface Control Document and the Use Cases Document. These are the baseline documents that drive all coding and testing activities. Development and testing processes are closely interrelated, and development activities don't end when items are moved into testing. Errors and/or deficiencies are returned cyclically to the developers for correction and unit testing before attempting the testing process again. Customization of the system

isn't complete until all system testing is completed, approved and accepted by DHHR.

PM023	4117	1	The solution rules/procedures should allow and enforce multiple service limits for different service ranges including, but not limited to:
PM024	5198	2	Applicable test cases
PM025	5199	2	Expected test results
PM026	5200	2	Others as defined by the Department

The Test Plan describes the overall strategy for testing, the processes and the tools used for test execution, management, and reporting for each test level. The approach taken for each test level describes the test methods to verify the business, technical, and operational elements of the project. The testing process identifies the items to be tested, test objectives, test schedules, entry and exit criteria, reporting requirements, evaluation criteria, defect resolution, and environment requirements. We describe the development methods for the test conditions, scenarios and scripts. We also provide test criteria for non-testable requirements. See Addendum C - Payer Integration Test Plan

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.

Our planning for testing and test traceability begins early in the project, during the Requirements Analysis Phase. A System Test Plan will be submitted to DHHR for approval after completion of the Requirements Definition Phase (aka Requirements Analysis Phase). See Addendum C - Payer Integration Test Plan

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.

Users have access to a sandbox environment where they can practice and test features, functions and processes without impacting live data.

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.

See Addendum C - Payer Integration Test Plan In general the scope of testing for the department will be focused on a) any data transmitted to Tellus and b) any data received from Tellus.

PM030	4131	1	The Vendor should provide the Department weekly reports of testing status, including, but not limited to:
PM031	5201	2	Metrics on the number of tests completed
PM032	5202	2	Number of deferred or canceled tests
PM033	5203	2	Results of the tests executed
PM034	5204	2	Defects identified by severity level
PM035	5205	2	Corrective actions taken
PM036	5206	2	Others as defined by the Department

The quality team at Tellus is ultimately responsible for testing the EVV solution. This testing includes developing the test plan, setting up test cases, and performing different levels of required testing, such as system integration testing and performance testing. Once testing

is complete, we will provide the results to DHHR as requested. See Addendum C - Payer Integration Test Plan

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.

Our approach in the implementation process is to ensure that the system is functionally sound and operationally stable before the pilot or soft launch process. Our implementation team, quality assurance and test teams work together to thoroughly "shake out" the system.

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.

A Soft Launch/Pilot testing process is an excellent way to mitigate risk in the rollout process. In a Soft Launch, constituents work together to ensure the system is designed to perform as required end to end. A cross-section of selected users including payers, providers, administrators, and direct care providers who are trained and will go-live prior to statewide roll-out. The EVV solution is used for "live" visits which are collected at the point-of-care and processed through the system. The direct care providers who are participating in this pilot process may also do paper timesheets, so that those results can be compared to the automated results.

PM039	4144	1	The Vendor should provide written test results of the Pilot Testing to the Department within an agreed upon timeframe.

Once transactions begin to flow through the system during the Soft Launch, as described in the system flow diagram, all of the data is checked for accuracy and expected results. This process involves all participants, ensuring that the EVV system is receiving and accepting the visit data; and that all external interfaces (including the Data Aggregator and MMIS) are functioning in accordance to the specifications.

PM040	4145	1	The Vendor should provide the Department official written notification of readiness for full production operations after completion of Pilot Testing.

Anticipated versus actual results from the Soft Launch are documented and provided to the State to certify the system is ready for rollout to the remainder of the state.

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.

Interface Testing will be performed in conjunction with DHHR. Our Interface Test Plan will be a component of our QA Test Plan submitted to DHHR for approval. Our integration testing and implementation strategy is supported by our internally tested checklist documenting activities and check points required to be performed by both Tellus and our integration partner.

PM042	3987	1	The Vendor should conduct interface testing with external electronic visit verification (EVV) data partners approved by the Department.

Any external EVV data partners will need to be identified during the Design Management phase of the project. Management of interface testing with any external EVV data partners will be managed by the Tellus Integrations Team and will be both approved by the Department and regularly reported on by the Tellus project manager.

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.

All testing and training environments provided to DHHR are included in the project cost.

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.

The UAT environment reflects all functionality of the production environment, so it is a critical step for establishing system readiness before moving the system into production. We will provide training to a core group of State staff users as required by the RFP. State staff will receive end-to-end system training with detailed information about our system development and deployment methodology before user acceptance testing (UAT). This approach will help us perform a comprehensive UAT. A separate training environment (independent of our UAT environment) will be utilized for training.

PM045	4788	1	The Vendor should create, use, and make available to the Department, representative samples for testing edits, business rules, and workflow processing.

Yes, Tellus will make applicable samples available as part of the design process.

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)

Yes, Tellus will coordinate with the department to define requirements for scrubbed test data that does not contain PHI as an integral part of the test planning.

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.

Yes, See Addendum C - Payer Integration Test Plan. Tellus writes Test Cases in Jira Test Manager and is willing to share these with the Department.

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)

Tellus ensures that web portal design is in accordance with Departments and federal regulations and guidelines as requested.

PM049	5227	1	The solution should be developed and implemented in accordance with the project work plan.

A Project Manager will be assigned to the DHHR project on a full-time basis for the duration of configuration and implementation, until the EVV system is successfully implemented and accepted by the State. The Project Manager will have the authority to make day-to-day project decisions for Tellus and be responsible for all project management activities, including maintaining the project plan over the life of the project and validating that we satisfy all contract requirements. The Project Manager will schedule and host meetings with DHHR Subject Matter Experts (SMEs) to review business organization and functions along with the organization, functions, and data of existing information systems relevant to this project, and will host other important meetings, assign staff to those meetings as appropriate, and provide an agenda for each meeting. The Project Manager will lead weekly status meetings, including monthly milestone meetings and will record and distribute the minutes upon request. The minutes will include key decisions along with closed, active and pending issues. The Project Manager will also participate in all other State, provider

and stakeholder meetings as requested.

PM050	5244	1	The Vendor should conduct the following types of testing in support of the solution:
PM051	5245	2	Unit testing
PM052	5247	2	Iterative functional testing
PM053	5248	2	System integration testing (SIT)
PM054	5249	2	Interface testing
PM055	5250	2	Regression testing
PM056	5251	2	End-to-end testing
PM057	5252	2	Security testing
PM058	5253	2	Performance testing
PM059	5254	2	Usability/Accessibility testing
PM060	5255	2	Browser testing
PM061	5256	2	User acceptance testing (UAT)
PM062	5257	2	Data conversion testing
PM063	5258	2	Operational readiness testing (ORT)
PM064	5259	2	Other testing as identified by the Department and/or Vendor

The following components of the Development Phase ensure delivery of a system that successfully meets the defined standards and provides all functionality.

Unit Testing. Every requirement or system function has a use case that is documented and coded. Coding only takes place after use cases are documented. We base unit tests on the detailed requirements specified in the use case.

Iterative functional testing – To be performed using both manual and automated methods per the test plan.

System integration testing (SIT)/ Data conversion testing

– To be performed primarily using manual methods per the test plan.

Functional Demonstration. Upon completion of system test activities, Tellus performs a functional demonstration of the EVV so the State can ensure solution design requirements meet or exceed expectations.

Interface Testing. The main focus of interface testing is the proper and accurate transmission of files between external systems and the EVV system to ensure interfaces are operationally ready and stable.

System Acceptance Testing. System acceptance testing enables the State to test system functionality and ensure all system design requirements are met. Tellus develops a system acceptance plan that complies with all testing requirements and test participants follow detailed scripts developed by Tellus and approved by DHHR.

Regression Testing. Full regression testing is performed before the system acceptance test to avoid unacceptable test results. System coding is prepared in accordance with specific State of Michigan requirements defined in the requirements document to ensure that all parties agree on the project's scope and deliverables. Unit, integration and full regression testing is performed once coding is complete to ensure the system is functioning according to documented requirements.

End-to-end testing – To be performed using both manual and automated methods per the test plan.

Security testing – To be performed using both manual and automated methods per the test plan. Includes automated static- and dynamic-code testing.

Performance/Stress Testing. Performance breaks down into two components: volume and stress. The purpose of volume testing is to determine that sufficient capacity exists to handle anticipated peak volumes. These volumes are derived from the current program transaction history with an upward adjustment for anticipated trends in increased caseload or additional programs. The purpose of stress testing is to determine the maximum capacity of the system configuration as a whole and is, therefore, a more destructive type of test where transactions are run at an escalating rate until the system indicates that the maximum rate has been or is about to be reached. Tellus performs both volume and stress tests to identify the system's capacity and to rigorously test the software and hardware components.

Usability/Accessibility testing – To be performed as part of 508 compliance testing.

Browser testing - All supported browser and operating systems to be tested using primarily automated testing methods.

User acceptance testing (UAT) – To be performed primarily by the department with Tellus support per the test plan.

Operational readiness testing (ORT) – Final testing to be performed by Tellus and the Department prior to production rollout. Includes go-to-market readiness.

Network Performance Testing. A network performance test of the EVV system communication networks is conducted to ensure the network is capable of handling projected transaction volumes in the required response times and error thresholds.

PM065	5260	1	The Vendor should be prepared to assist the Department, as necessary, with User acceptance testing (UAT).

We will provide training to a core group of State staff users as required by the RFP. State

staff will receive end-to-end system training with detailed information about our system development and deployment methodology before user acceptance testing (UAT). This approach will help us perform a comprehensive UAT.

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.

Tellus will perform UAT to the extent possible without Department resources, but a portion of UAT includes testing of Department systems that will receive data from Tellus. This testing must be performed by the Department.

PM067	5262	1	The Vendor should complete regression testing subsequent to, but not limited to, the following:
PM068	5263	2	Deployment of new solution components
PM069	5264	2	Integration of each solution component into the primary solution
PM070	5265	2	Every migration of new build versions to each test environment
PM071	5266	2	Solution fixes
PM072	5267	2	Solution patches
PM073	5268	2	Solution releases
PM074	5269	2	Others as defined by the Department

Yes, Tellus will perform manual and automatic regression testing prior to every release.

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.

Yes, we expect regression testing to include SIT testing.

PM076	5271	1	The Vendor should obtain approval from the Department on which scenarios should be used for regression testing.

Yes, regression testing details will be addressed as part of the Test Plan.

PM077	5272	1	The Vendor should utilize end-to-end test cases in support of regression testing.

Yes, regression testing details will be addressed as part of the Test Plan.

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)

Yes, Tellus performs privacy and security testing that includes but is not limited to manual testing, automated testing, static code testing, and dynamic code testing prior to every release.

PM079	5274	1	The Vendor should propose testing scenarios and/or cases to the Department for their approval.

Test Plans will be submitted to DHHR for approval after completion of the Requirements Definition Phase (aka Requirements Analysis Phase).

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.

Our Performance/Stress Testing is broken down into two components: volume and stress. The purpose of volume testing is to determine that sufficient capacity exists to handle anticipated peak volumes. These volumes are derived from the current program transaction history with an upward adjustment for anticipated trends in increased caseload or additional programs. The purpose of stress testing is to determine the maximum capacity of the system configuration as a whole and is, therefore, a more destructive type of test where transactions are run at an escalating rate until the system indicates that the maximum rate has been or is about to be reached.

PM081	5277	1	The Vendor's performance testing should occur on a production ready version of the solution.

Tellus performs both volume and stress tests in NAME OF ENVIRONMENT to identify the system's capacity and to rigorously test the software and hardware components.

PM082	5278	1	The solution's performance testing environment should mirror the final production solution specifications.

Yes, Tellus UAT and Staging environments have the same topology as our production environment.

PM083	5279	1	The Vendor should perform usability/ accessibility testing for various types of users, including, but not limited to:
PM084	5280	2	Internal users
PM085	5281	2	External users
PM086	5283	2	Users with limited computer skills
PM087	5284	2	New user registration
PM088	5286	2	Users with disabilities

PM089	5287	2	Others as defined by the Department

Yes, usability and accessibility testing are carried out by third-party vendor as part of 508-compliance certification.

PM090	4133	1	The Vendor should conduct an Operational Readiness Review (ORR) prior to statewide implementation of the solution.

Yes, Tellus considers go-to-market/ Operational Readiness to be a parallel track on every implementation with the culmination in a set of Operational Readiness Review (ORR) sessions prior to production release.

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.

Tellus will work with DHHR to determine the anticipated volume for 30 calendar days of production-capacity and included a volume/stress test of that magnitude as part of our ORR to demonstrate the solution and Tellus staff is prepared for full production.

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).

Tellus will document and propose solutions and timeframes for corrective actions to all issues, problems and defects identified through the ORR.

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.

Tellus will prepare and submit to DHHR an ORR Report demonstrating Tellus and Tellus EVV are ready to begin operations.

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:
PM095	4969	2	Correct the report
PM096	4970	2	Verify the report
PM097	4971	2	Distribute or re-distribute the report
PM098	4972	2	Others actions as defined by the Department

Tellus will correct any report errors identified and correct the report with an agreed upon timeframe as defined in the Change Management Plan. At a minimum, actions will include correcting, verifying and distributing or re-distributing the report.

PM099	4089	1	The Vendor should assist the Department with specialized research and reporting as requested.

Tellus will assist DHHR with specialized research and reporting as defined.

PM100	4787	1	The Vendor should be able to test edits, business rules, and workflow processing and report on results.

Yes, business rule testing is an integral part of the test plan.

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.

See Addendum F - Vendor Transition or Termination Policy

PM102	4448	1	The Vendor should obtain Department approval of all scripts prior to implementation that will be used in the Technical Call Center.

Tellus will obtain DHHR approval of all Technical Call Center scripts prior to implementation.

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.

Yes, Tellus publishes a catalogue all any third-party solutions that are an integrated part of the Tellus solution.

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.

Information gathered during this phase of the engagement will be used to create the Functional Requirements Document, which will be presented to the State for review and approval.

Tellus will coordinate with the department to organize a series of Joint Application Development (JAD) sessions for this purpose.

The Functional Requirements Document will serve as the foundation for the Detailed System Design Document, which will describe how our EVV solution addresses the State's requirements.

PM105	522	1	The Vendor should maintain a requirements traceability matrix (RTM) throughout the lifecycle of the project.

After configuration or coding, the testing team verifies the deliverables of the implementation phase against requirements using our Requirements Traceability Matrix (RTM). The testing team follows the Software Testing Lifecycle (STLC) which is similar to the development cycle adopted by the development team.

PM106	5230	1	The Vendor should provide all stakeholders identified by the Department access to the requirements traceability matrix (RTM).

Yes, Tellus will make the RTM available to any interested stakeholders.

PM107	5231	1	The Vendor should document in the requirements traceability matrix (RTM) where each requirement is accounted for, including, but not limited to:
PM108	5232	2	Design documentation
PM109	5233	2	Code modules
PM110	5234	2	Test conditions
PM111	5235	2	Test scenarios
PM112	5236	2	Test cases
PM113	5237	2	Certification criteria
PM114	5238	2	Medicaid Information Technology Architecture (MITA) business areas and processes

- Adapting the design and development in a timely manner to meet any approved changes in requirements that occur during the Implementation Phase.
- Performing unit, functional, integration, system and regression testing.

During the Execution & Build Phase, we use a time-tested, refined methodology for software development that includes thorough testing and detailed documentation to prepare and validate all systems for live operations. All system testing, as well as development of training materials, occurs during this phase. This process ensures that the EVV solution is configured and tested according to all applicable State and Federal regulations as defined and mutually agreed upon during the Planning & Design Phase, and as identified in the JAD session.

All development activities, including testing, are driven by user requirements, system specs, the Interface Control Document and the Use Cases Document. These are the baseline documents that drive all coding and testing activities. Development and testing processes are closely interrelated, and development activities don't end when items are moved into testing. Errors and/or deficiencies are returned cyclically to the developers for correction and unit testing before attempting the testing process again. Customization of the system isn't complete until all system testing is completed, approved and accepted by the State.

The following components of the Development Phase ensure delivery of a system that successfully meets the defined standards and provides all functionality.

- **Unit Testing.** Every requirement or system function has a use case that is documented and coded. Coding only takes place after use cases are documented. We base unit tests on the detailed requirements specified in the use case.

- **Functional Demonstration.** Upon completion of system test activities, Tellus performs a functional demonstration of the EVV so the State can ensure solution design requirements meet or exceed expectations.

- **Interface Testing.** The main focus of interface testing is the proper and accurate transmission of files between external systems and the EVV system to ensure interfaces are operationally ready and stable.

- **System Acceptance Testing.** System acceptance testing enables the State to test system functionality and ensure all system design requirements are met. Tellus develops a system acceptance plan that complies with all testing requirements and test participants follow detailed scripts developed by Tellus and approved by the State of Michigan.

- **Regression Testing.** Full regression testing is performed before the system acceptance test to avoid unacceptable test results. System coding is prepared in accordance with specific State of Michigan requirements defined in the requirements document to ensure that all parties agree on the project's scope and deliverables. Unit, integration and full regression testing is performed once coding is complete to ensure the system is functioning according to documented requirements.

- **Performance/Stress Testing.** Performance breaks down into two components: volume and stress. The purpose of volume testing is to determine that sufficient capacity exists to handle anticipated peak volumes. These volumes are derived from the current program transaction history with an upward adjustment for anticipated trends in increased caseload or additional programs. The purpose of stress testing is to determine the maximum capacity of the system configuration as a whole and is, therefore, a more destructive type of test where transactions are run at an escalating rate until the system indicates that the maximum rate has been or is about to be reached. Tellus performs both volume and stress tests to identify the system's capacity and to rigorously test the software and hardware components.

- **Network Performance Testing.** A network performance test of the EVV system communication networks is conducted to ensure the network is capable of handling projected transaction volumes in the required response times and error thresholds.

- **IVR Testing.** The IVR application is thoroughly tested to ensure the system properly accepts, processes and transfers calls while properly handling expected call volume.

- **EVV Documentation.** Tellus provides complete documentation for our EVV system, which is updated across the life of the project, and includes Administrative System Documentation accompanied by a Training Manual that encompasses complete Administrative System Functionality; and a Reports Manual describing all

standard and State-specific reports, as well as a description of the data files furnished to the State for internal report generation.

f. Implementation Plan Installation / Go-Live

Tellus completes the installation objectives of the Implementation Phase by:

Assisting the State of Michigan in creating User Acceptance Test (UAT) cases and in performing UAT of the system.

Providing a deployment plan leading to successful implementation of EVV.

Providing initial user training, staff preparation for operations, build-out of operations infrastructure and related supporting activities 30 days prior to the operation start date.

Our approach in the implementation process is to ensure that the system is functionally sound and operationally stable before the pilot or soft launch process. Our implementation team, quality assurance and test teams work together to thoroughly "shake out" the system.

A Soft Launch is always an excellent way to mitigate risk in the rollout process. In a Soft Launch, constituents work together to ensure the system is designed to perform as required end to end. A cross-section of selected users including payers, providers, administrators, recipients and direct care providers are trained and will go-live prior to statewide rollout. The EVV solution is used for "live" visits which are collected at the point-of-care and processed through the system. The direct care providers who are participating in this pilot process may also do paper timesheets, so that those results can be compared to the automated results.

Once these transactions begin to flow through the system, as described in the system flow diagram, all of the data is checked for accuracy and expected results. This process involves all participants, ensuring that the EVV system is receiving and accepting the visit data; and that all external interfaces (including the Data Aggregator and MMIS) are functioning in accordance to the specifications. Anticipated versus actual results are documented and provided to the State to certify the system is ready for rollout to the remainder of the state.

Another benefit of the Soft Launch is that adjustments can be made in the training programs if something seems difficult or not intuitive to the pilot team. Adjustments to the

web-based console and the reporting system can also be made once the results are analyzed. Reporting "dashboards" can also be enhanced during this phase to monitor any specific issues encountered during the pilot. The live data flowing through the various integration programs is also a good test of the bi-directional communication processes.

At this point, the State has received all feedback, and we are ready for a Statewide launch. With the lessons learned by all parties, the remaining users should experience a smooth and positive start to their EVV program.

During all phases of the implementation, all necessary artifacts required for mandatory go-live readiness are collected and stored. Additional assistance required from the State may be requested during the regular, established meetings and/or communication methods to ensure timely response and/or approval of the stated assistance request. Our experience is that timely assistance is very beneficial during the initiating and planning phases of the project.

3.1 Requirements Analysis and Solution Design Methodology

Instructions: 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.

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 Vendorto create usage scenarios and detailed business process workflows.

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.

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.

The solution design and its multiple components should be developed in conjunction with the Project Work Plan as follows:

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.

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.

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.

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.

The Vendor's proposed approach to requirements analysis and solution design should also include detail on the following:

Process for identifying and resolving gaps between the Vendor's and DHHR's understanding of an RFP specification.

How the solution's design will include collaborative design with functional and technical subject matter experts.

*How the Vendor intends to obtain DHHR approval on **RFP** specifications.*

Description of how the proposed solution will fulfill the Medicaid Information Technology Architecture (MITA) requirements.

Design documentation for all those project deliverables delivered during the Solution Planning and Solution Design, Testing, and Operational Readiness taskgroups.

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.

Solution Design is arguable the most important part of the engagement. Making sure requirements are properly captured, understood and agreed upon is the first step to building and deploying a successful program. Tellus completes the design objectives of the Implementation Plan by:

- Conducting discovery activities and requirements development, beginning immediately after the award of the Contract
- Conducting familiarization activities to better understand the needs of the Medicaid Enterprise
- Building the key planning documents for the Design Implementation Phase
- Performing verification of deliverables
- Designing the EVV system for, and receiving verification by, DHHR in joint meetings

To confirm our understanding of requirements provided by DHHR, Tellus will develop and submit for review the following deliverables during the Solution Planning Phase of the Engagement:

- Requirements Management Plan
- Requirements Specification Document
- Requirements Traceability Matrix
- System Requirement Document/User Stories
- Detailed System Design Document
- Configuration Management Plan
- Database Design Document & Data Models
- Capacity Plan
- Modularity and Reusability Plan
- Data Management Plan
- Data Security, Privacy & Confidentiality Plan

This body of documents prepared, reviewed and agreed upon will serve as the foundation for the development of the solution. These are living documents that will be updated through the course of the development of the solution, through testing and up to user acceptance certification as requested through the Change Management Process.

3.2 Solution Development Methodology

Instructions: 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.

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.

The Vendor's proposal should present a narrative description of the Vendor's proposed approach to solution development, including the Vendor's proposed:

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:

Regular system maintenance, performance optimization, resource capacity utilization, capacity planning, and capacity expansion.

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.

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.

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.

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.

Methodology and approach to ensure that the developed solution meets design criteria.

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.

Tellus completes the development objectives of the engagement by:

- Developing and constructing the system, based on approved requirements
- Adapting the design and development in a timely manner to meet any approved changes in requirements that occur
- Performing unit, functional, integration, system, regression testing and user acceptance testing

During the Execution & Build Phase, we use a time-tested, refined methodology for software development that includes thorough testing and detailed documentation to prepare and validate all systems for live operations. All system testing, as well as development of training materials, occurs during this phase. This process ensures that the EVV solution is configured and tested according to all applicable State and Federal regulations as defined and mutually agreed upon during the Planning & Design Phase, and as identified in the JAD session.

All development activities, including testing, are driven by user requirements, system specs, the Interface Control Document and the Use Cases Document. These are the baseline documents that drive all coding and testing activities. Development and testing processes are closely interrelated, and development activities don't end when items are moved into testing. Errors and/or deficiencies are returned cyclically to the developers for correction and unit testing before attempting the testing process again. Customization of the system isn't complete until all system testing is completed, approved and accepted by DHHR.

3.3 Data Conversion Strategy, Approach, and Timeline

Instructions: 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).***

The Vendor's proposal should also describe how the Vendor will ensure data integrity and consistency through all phases of the project.

Data Integration is a core competency for Tellus, we understand the current Operating

Environment requires sharing data across platform solutions and that data integrity is the key to successfully managing Medicaid programs. Tellus is currently integrated with MMIS, Agency Management and other third-party vendor systems as depicted in the graphic below.

Successfully developing and managing a series of bi-directional integrations will begin at the Project Initiation Phase by developing a Data Conversion Plan and a System Integration Plan. As the Solution is defined, the plans will evolve into an Interface Inventory and supporting Test Cases. Interface testing focuses on the proper and accurate transmission of files between external systems and the EVV system to ensure interfaces are operationally ready and stable.

Tellus will test each Interface and submit Data Conversion and System Integration Test Results prior to the Deployment of the EVV platform.

3.4 Testing

Instructions: 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.

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.

The DHHR defines the types of testing as follows:

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.

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.

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.

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.

Interface Testing: Interface testing ensures the completeness of interface development and the readiness of developed interfaces for integration in the wider system.

Regression Testing: Regression testing assesses the integrity of the solution subsequent to the deployment of new solution components and/or fixes.

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.

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.

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.

Usability/Accessibility Testing: Usability testing ensures the solution user interface design takes into account usability considerations for its target user groups.

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.

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.

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.

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.

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.

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:

All aforementioned testing types, as well as any others the Vendor plans to deploy

Timing for execution of each testing type

Usage of tools the Vendor proposes be used in support of each testing type

Testing environments to be used in support of each testing type, and for all necessary testing activities

Validating the traceability of requirements throughout the full testing process

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.

The Vendor's proposal should also present a narrative description that includes the following:

Approach to completion of the Solution Design, Testing, and Operational Readiness task group's testing-related deliverables.

Approach to obtaining DHHR's approval of the testing-related project milestones including the proposed acceptance criteria for each milestone.

Approach to:

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

Developing test cases and scripts to thoroughly test system functionality

Supplying documentation of each testing type

Preparing data for each testing type

Details on the support the Vendor intends to supply during UAT, such as the Vendor's approach to:

Developing the UAT Plan, scripts, cases, timeline, and supporting processes

Preparing test data

UAT results analysis, identification of defect severity, and defect resolution

Defect tracking, repair, and reporting

UAT final report that includes:

A written certification letter certifying that UAT was successfully completed

A list of all defects and issues

A list of all resolved critical defects and/or issues

The Vendor's proposal should also include detail on the approach to ORT including details on:

ORT approach

ORT final report that includes:

A written certification letter certifying that UAT was successfully completed

A list of all defects and issues

A list of all resolved critical defects and/or issues

Tellus provides complete documentation for our EVV system, which is updated across the life of the project, and includes Administrative System Documentation accompanied by a Training Manual that encompasses complete Administrative System Functionality; and a Reports Manual describing all standard and State-specific reports, as well as a description of the data files furnished to the State for internal report generation.

This documentation is initiated during the solution planning phase and is the foundation for unit tests conducted throughout the system design phase as well as the development of user acceptance test cases conducted at defined milestones and at the end of the development phase.

The following components of the Development Phase ensure delivery of a system that successfully meets the defined standards and provides all functionality.

- **Unit Testing.** Every requirement or system function has a use case that is documented and coded. Coding only takes place after use cases are documented. We base unit tests on the detailed requirements specified in the use case.
- **Functional Demonstration.** Upon completion of system test activities, Tellus performs a functional demonstration of the EVV so the State can ensure solution design requirements meet or exceed expectations.
- **Interface Testing.** The main focus of interface testing is the proper and accurate transmission of files between external systems and the EVV system to ensure interfaces are operationally ready and stable.
- **System Acceptance Testing.** System acceptance testing enables the State to test system functionality and ensure all system design requirements are met. Tellus develops a system acceptance plan that complies with all testing requirements and test participants follow detailed scripts developed by Tellus and approved by the State of Michigan.
- **Regression Testing.** Full regression testing is performed before the system acceptance test to avoid unacceptable test results. System coding is prepared in accordance with specific State of Michigan requirements defined in the requirements document to

ensure that all parties agree on the project's scope and deliverables. Unit, integration and full regression testing is performed once coding is complete to ensure the system is functioning according to documented requirements.

- **Performance Load/Stress Testing.** Performance breaks down into two components: volume and stress. The purpose of volume testing is to determine that sufficient capacity exists to handle anticipated peak volumes. These volumes are derived from the current program transaction history with an upward adjustment for anticipated trends in increased caseload or additional programs. The purpose of stress testing is to determine the maximum capacity of the system configuration as a whole and is, therefore, a more destructive type of test where transactions are run at an escalating rate until the system indicates that the maximum rate has been or is about to be reached. Tellus performs both volume and stress tests to identify the system's capacity and to rigorously test the software and hardware components.
- **Network Performance Testing.** A network performance test of the EVV system communication networks is conducted to ensure the network is capable of handling projected transaction volumes in the required response times and error thresholds.

Once User Acceptance Testing is complete, the UAT results and Letter of Completion will be delivered to DHHR and Operational Readiness Test Scripts and their Results will move the project to the Deployment Phase.

4 Deployment Methodology

Instructions: 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:

Implementation/Rollout Planning

Implementation Methodology and Timeline

Issues, Challenges, and Risks

Lessons Learned

See our response to each component in the appropriate section below:

4.1 Implementation/Rollout Planning

Instructions: The Vendor's proposal should describe the Vendor's methodology, tools, and techniques for implementation/rollout planning. The Vendor should include what specific staging, readiness, and deployment techniques it will use to determine the proper sequencing of deployment processes and functions required for successful implementation.

The Vendor's proposal should include, but not be limited to, details on its approach and methodology for the following:

Completing all Solution Deployment task group-related deliverables

Obtaining approval of all Solution Deployment task group-related deliverables and milestones

Completing operational readiness and operational readiness testing (ORT)

Documenting emergency back-out strategy

Completing Pilot testing

Confirming stakeholder readiness for new solution implementation

The Vendor's proposal should also include details on its approach to supporting and/or supplying:

System documentation

User documentation

Reports

Report distribution schedule

Production environment, including the final production schedule

Data conversion

Pre-implementation training

Updates to project management plans for operations

Tellus begins Deployment Rollout Planning during the Project Initiation phase of the engagement. Each of the deliverables associated with Solution Deployment is incorporated into our project team along with a deliverable date and the Tellus resource responsible for delivering that artifact.

Each phase prior to the deployment of the solution must be completed with the end goal in mind, deploying an EVV solution that meets the goals and objectives of DHHR. To accomplish that the following activities supported by the appropriate documentation must be planned, refined and executed throughout the engagement:

- Stakeholders are prepared to begin using EVV to verify visits and submit claims
  - Operations Change Management Plan
  - Operational Milestone Review
  - Report Distribution Schedule
  - System & User Documentation
  - Training Materials
  - Training Report
  - Training Schedule
  - Training Sessions
- EVV solution is transitioned to production, supporting deliverables include
  - Cutover Play Book
  - Federal Review Supporting Documentation
  - Production Screenshots, Reports & Data to Certify
  - Implementation Certification Letter
  - Implementation Plan
  - Solution Health Monitoring Plan
  - System Operations Plan
  - Turnover & Closeout Management Plan

Prior to Production Rollout, initial user training, staff preparation for operations, build-out of operations infrastructure and related supporting activities must be completed.

Our approach in the implementation process is to ensure that the system is functionally sound and operationally stable before the pilot or soft launch process. Our implementation team, quality assurance and test teams work together to thoroughly "shake out" the system.

A Soft Launch is always an excellent way to mitigate risk in the rollout process. In a Soft Launch, constituents work together to ensure the system is designed to perform as required end to end. A cross-section of selected users including payers, providers, administrators, recipients and direct care providers are trained and will go-live prior to statewide rollout. The EVV solution is used for "live" visits which are collected at the point-of-care and processed through the system. The direct care providers who are participating in this pilot process may also do paper timesheets, so that those results can be compared to the

automated results.

Once these transactions begin to flow through the system, as described in the system flow diagram, all of the data is checked for accuracy and expected results. This process involves all participants, ensuring that the EVV system is receiving and accepting the visit data; and that all external interfaces (including the Data Aggregator and MMIS) are functioning in accordance to the specifications. Anticipated versus actual results are documented and provided to the State to certify the system is ready for rollout to the remainder of the state.

Another benefit of the Soft Launch is that adjustments can be made in the training programs if something seems difficult or not intuitive to the pilot team. Adjustments to the web-based console and the reporting system can also be made once the results are analyzed. Reporting "dashboards" can also be enhanced during this phase to monitor any specific issues encountered during the pilot. The live data flowing through the various integration programs is also a good test of the bi-directional communication processes.

At this point, DHHR will have received all feedback, and we are ready for a Statewide launch. With the lessons learned by all parties, the remaining users should experience a smooth and positive start to their EVV program.

During all phases of the implementation, all necessary artifacts required for mandatory go-live readiness are collected and stored. Additional assistance required from the State may be requested during the regular, established meetings and/or communication methods to ensure timely response and/or approval of the stated assistance request.

4.2 Implementation Methodology and Timeline

Instructions: The Vendor's proposal should describe an effective implementation and deployment strategy to meet DHHR's specifications and help ensure State compliance with mandatory EVV deadlines defined in the Cures Act.

*The Vendor's Initial Work Plan and work breakdown structure (WBS) in **Attachment 5: Initial Work Plan** should include a sufficient level of detail to show the tasks and phasing strategy to deliver full solution functionality and the proposed implementation timing for both PCS and HHCS.*

Please refer to Attachment 5 and related Addendums to review the draft of our Initial Work Plan and WBS.

4.3 Issues, Challenges, and Risks

Instructions: DHHR is interested in any information that may help identify issues, clarify the specifications, reduce risk of the procurement, and identify issues and challenges of designing and implementing the proposed solution.

The Vendor's proposal should highlight any concerns or recommendations in this section.

Tellus is confident in our ability to develop a successful EVV platform with DHHR. Change always presents challenges but with committed partnerships challenges, issues and risks are recognized, discussed and overcome.

4.4 Lessons Learned

Instructions: DHHR would find it helpful to understand what the Vendor sees as the successes and primary challenges in the implementation of similar systems. In order to gain this insight, DHHR would like to draw upon the Vendor's experiences with similar projects.

The Vendor's proposal should describe any "lessons learned" from the Vendor's relevant experience and how those lessons learned will impact the Vendor's approach to this project.

The modular architecture for Tellus EVV and the rules hierarchy were developed based on business requirements gathered to construct a versatile EVV platform for our clients. The rules and configurations continue to be updated, as required, based on lessons learned, provider feedback and refinement of claims adjudication processes and details.

Having fully deployed our solution for multiple payers, we bring to future deployments the benefit of lessons learned along the way. Key lessons learned during previous engagements throughout program design, development, deployment and operations and maintenance phases include the following:

- Quality of member care trumps all other considerations when establishing business rules, policies, and procedures.

- Provider adoption requires consistent, frequent outreach and training.
- Providers are extremely knowledgeable about program details and valuable sources of information.
- Access to appropriate program and technical client resources is a significant key to success.
- A soft launch with a subset of providers and a limited retention of current claims processing capability is important to test business rules, configuration and integrations without penalizing providers.
- Curious, helpful, motivated Customer Support resources are a huge asset to program integrity and technical innovation.

Innovative techniques and functionality we developed and implemented as a result of these learnings include:

- Refinement of the mobile app user interface to incorporate bigger fonts and buttons, consistent colors throughout the app and reduced number of steps to complete the required workflow.
- Multi-payer support because many direct attendants work for more than one provider, and many providers are members of more than one payer network.
- Customized Consumer-Directed Services (CDS) module to support the unique requirements of that community.
- Modern, modular tools to better support the following EVV program functionality:
  - Aggregation o Integration
  - Dashboard Visualization & Customization o Reporting
  - Business Intelligence Rules

5 TRAINING

Instructions: *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:*

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.*

Approach to development, maintenance, and implementation of the Training Management Plan, including methodologies addressing:

Assessment of internal and external training needs, including gap analysis

Approach to user training, supporting all business processes as identified in the RFP

Delivery of end-user training throughout the solution's implementation

Development and use of online tutorials, online help, online policy and procedure manuals, and hard copy user manuals for the delivery of training

Development and use of live, web seminar, and video-based training

The target audiences for training, including ***DHHR*** *staff, Vendor staff, clients, providers, and third-party stakeholders that work in the system*

Plan to provide and/or leverage existing DHHR training facilities to perform end-user training detailed in this section

Tools that the Vendor will use to support training

The planned curriculum for each system user role and audience

Initial training schedule

Version control and maintenance of training documentation

Training evaluation, including the use of evaluation survey tools to determine whether the trainings produced the expected results

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

Approach to "train-the-trainer" activities during the Operations phase

Approach to role-based training during both implementation, and maintenance and operations

Approach to development of training materials

Approach to training evaluations

At Tellus, our EVV implementation is supported by a thorough and accessible training program designed to meet the needs of individual users including those with disabilities. Accommodations adhere to all State and Federal laws, rules, regulations and guidelines. Training sessions and related materials are available in English and Spanish. Training

incorporates all the following elements at the appropriate level for the User role that the training session is designed for:

- System access and log-on
- Data entry and updates
- Visit capture and validation
- Visit maintenance/updates to EVV visit transactions
- Clock-in/Clock-out methods
- Access and creation of reporting
- Customer Service (system troubleshooting, issue reporting, complaints, etc.)

Tellus will track completion of training for all users and report data in the EVV Vendor Monthly Performance report and at the request of the State of Michigan. User training is role-based, with sessions and materials geared to these roles:

- Direct care providers receive hands-on, step-by-step instruction on use of the mobile app and alternative verification methods. They also act as trainers, and we provide training on how to instruct and immediately support recipients during the sign-off phase.
- Consumer-Directed Services Employers are trained to use the Consumer-Directed Console and related timesheet functionality.
- Fiscal Management Services DHHR staff are trained to use the FMS portal as well as trained how to provide instruction and immediate support for Consumer-Directed Employers and their direct care providers.
- Provider DHHR Administrators receive in-depth training on the Administrator Console, the Claims Console and the Mobile App so they can assist employees and peers on use of the system and troubleshoot minor issues on site.
- Individuals in Billing and Financial roles receive training related to use of the Claims Console and the reporting features available within it.
- State Staff receive high level end-to-end system training as well as hands-on, step-by-step instruction for use of the State level Tellus EVV Console.
- Managed Care Organizations users receive hands-on, step-by-step instruction for use of the MCO level Tellus EVV Console.
- Recipients are engaged through focus groups initially to gain understanding of outreach and training needs. Our outreach campaigns are designed to raise awareness and promote the benefits of the EVV system. Online training is provided to recipients, particularly for consumer-directed members, to support them in navigating the system.

Direct care providers act as supporting trainers in explaining the sign-off phase of the process to recipients.

Training is delivered in a multi-modal approach that includes:

- Live, face-to-face training. During the initial implementation, a series of regional face-to-face, hands-on training events are scheduled in the months and weeks leading up to the State of Michigan's Go Live date. These training events include a variety of sessions covering topics designed to address the needs of State users, DHHR administrators and direct care providers, including special training for recipients and their designated representatives who are enrolled in a consumer-directed program.
- Live, interactive, role-based webinars. Trainers walk attendees through step-by-step instruction, based on their role as noted above. Attendees are encouraged to submit specific training or demo requests in advance of the session so live training can be tailored to the audience's needs. A question and answer session is held during the last 10 minutes of each session. If time doesn't allow for all questions to be asked and answered during the session, attendees can submit questions via email for individual response and follow-up.
- Online training and support center. Our easy-to-use, easy-to-access web-based training and support center offers a centralized location for access to training resources including user guides, FAQs, recorded training sessions, video tutorials and easy access to request additional support from our help desk.
- Sandbox Environment. Users have access to a sandbox environment where they can practice and test features, functions and processes without impacting live data.
- Train the Trainer. We encourage the State and provider agencies to identify certain individuals to receive in-depth training and serve as the resident experts at their site. These individuals play an important role in helping onboard new users and act as a liaison between Tellus training staff and their site to ensure their needs are always met in a timely fashion.
- Ongoing Refresher Courses and New Feature Training. Training sessions are available on an ongoing basis for new users and anyone needing a refresher. Tellus training staff also provides outreach and training to coincide with the release of new features and functionality.
- Printable Reference Materials. Reference materials included on the online training and support center are easily printable or downloadable.

- Simple User Guides and Tip Sheets. These guides will be shared with direct care providers and recipients to support their ongoing effective use of the system.
- Ongoing Communications. We also provide regular, ongoing communications with users to communicate tips and tricks, upcoming release information, important dates and other pertinent information. This includes offline means of communication, such as targeted mail campaigns as well as an active social media effort.

Tellus provides complete documentation for our EVV system, which is updated across the life of the project, and includes Administrative System Documentation accompanied by a Training Manual that encompasses complete Administrative System Functionality; and a Reports Manual describing all standard and State-specific reports, as well as a description of the data files furnished to the State for internal report generation.

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:
TN002	5176	2	Members or Legal Representative
TN003	5177	2	Direct Care Workers
TN004	5178	2	Provider Agencies
TN005	5197	2	The Department
TN006	5179	2	Other as defined by the Department

In our experience, Outreach should begin early in the planning process and continue post-deployment during the operational phase of the project. We communicate with all relevant audiences specified by DHHR. To lay the proper groundwork to facilitate ongoing communications, Tellus recommends the following:

1. Maintain a list of participating providers including contact information particularly phone numbers and email addresses.

2. Outreach to the community with multiple email blasts for provider, member and direct care provider alerts as well as care managers.

3. Email all affected EVV users anytime any functional changes to the system occur, which should include the changes made and the release notes.

4. For global communications and training sessions, Tellus recommends the State of Michigan have a beta group review communication materials and training information to provide feedback and advice prior to release.

TN007	3974	1	The Vendor should provide training at the time of registration.

Tellus will develop a training plan and schedule to support users throughout the implementation process in a variety of modalities. Training at the time of registration can be accommodated.

TN008	4146	1	The Vendor should collaborate with the Department and the stakeholder community to develop strategies to train members receiving services.

Tellus will collaborate with DHHR and the stakeholder community to develop strategies to train members receiving services. This training is likely to vary among programs and service delivery models.

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.

During the initial implementation, a series of regional face-to-face, hands-on training events are scheduled in the months and weeks leading up to the DHHR Go Live date. These training events include a variety of sessions covering topics designed to address the needs of State users, DHHR administrators and direct care providers, including special training for recipients and their designated representatives who are enrolled in a consumer-directed program.

We encourage the State and provider agencies to identify certain individuals to receive in-depth training and serve as the resident experts at their site. These individuals play an important role in helping onboard new users and act as a liaison between Tellus training staff and their site to ensure their needs are always met in a timely fashion.

TN010	4152	1	The Vendor should provide written training materials for both in-person and web-based training options.

Our easy-to-use, easy-to-access web-based training and support center offers a centralized location for access to training resources including user guides, FAQs, recorded training sessions, video tutorials and easy access to request additional support from our help desk.

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.

Tellus will submit training materials to DHHR for review and approval at least 5 days prior to the date of the first training session.

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)

Our EVV implementation is supported by a thorough and accessible training program designed to meet the needs of individual users including those with disabilities. Accommodations adhere to all State and Federal laws, rules, regulations and guidelines.

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 sessions and related materials are available in English and Spanish.

TN014	4156	1	The Vendor should obtain independent verification of the accuracy of all translations made pursuant to language and accessibility requirements.

User documents are published in both English and Spanish. We will verify accuracy of all translations.

TN015	4158	1	The Vendor should provide web-based training available to users throughout the life of the solution.

Our easy-to-use, easy-to-access web-based training and support center offers a centralized location for access to training resources including user guides, FAQs, recorded training sessions, video tutorials and easy access to request additional support from our help desk.

TN016	4160	1	The Vendor should provide a detailed approach to user training with respect to solution modifications.

Training sessions are available on an ongoing basis for new users and anyone needing a refresher. Tellus training staff also provides outreach and training to coincide with the release of new features and functionality

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.

Tellus will track completion of training for all users and report data in the EVV Vendor Monthly Performance report and at the request of DHHR.

TN018	4162	1	The Vendor's training records should be included in the data available for reporting.

Tellus will compile training records and include them in the data available for reporting based on DHHR specifications.

TN019	4168	1	The Vendor should provide a user manual to all users.

Our user manuals are located in our online training and support center and are easily printable or downloadable.

TN020	4169	1	The user manual should be subject to Department approval.

The user guides are currently universal for all users of the Tellus EVV System. Any training materials (PowerPoint decks or other materials) that are unique to the West Virginia program will be subject to Department approval.

TN021	4170	1	The user manual should be available online and in hard copy upon request of the user.

Reference materials included on the online training and support center are easily printable or downloadable.

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)

User manuals are designed to meet the needs of individual users including those with disabilities. Accommodations adhere to all State and Federal laws, rules, regulations and guidelines.

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)

The user manual can be translated into any language specified by DHHR.

TN024	5289	1	The solution should support workforce security awareness through such methods including, but not limited to:
TN025	5290	2	Security reminders (at login or screen access)

TN026	5291	2	Training reminders
TN027	5292	2	Online training capabilities
TN028	5293	2	Training tracking
TN029	5294	2	Others as defined by the Department.

Tellus supports workforce security awareness including:

- Security reminders
- Training reminders
- Online training instructions
- Training tracking
- Custom requirements outlined by DHHR can be accommodated.

6 CMS CERTIFICATION

Instructions: 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.

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.

Tellus software application architecture and processes support the Seven Standards and Conditions advocated by CMS as follows:

1. **Modularity Standard:** Tellus EVV is comprised of five major modules, or components, that operate together or individually. The modules work seamlessly together in a runtime environment employing loosely coupled services. Real-time rendered service data is available for claims pre-adjudication and 837 submission to MMIS on the day services are completed. Payer adjudication data can be imported to EVV and made available to providers as soon as the payer transmits the information to Tellus. Tellus can accept standard 835 or proprietary data formats.

2. **MITA Condition:** Tellus will assist the State in documenting "As-Is" and "To-Be" environments of business, information and technical capabilities demonstrating an increasing MITA maturity level, complying with MITA 3.0. Tellus will also strive to identify and recommend opportunities to leverage the reuse of health care technologies within the State and among other states.

3. **Industry Standards Condition:** Tellus EVV is fully compliant with the following standards: a. Health Insurance Portability Act of 1996 (HIPAA) b. Health Information Technology for Economic and Clinical Health Act (HITECH) c. National Institute of Standards and Technology (NIST) Special Publication (SP) 800 d. Section 508 of the Rehabilitation Act, Americans with Disabilities Act (ADA) e. Federal Civil Rights Laws f. Section 1104 of the Affordable Care Act g. Section 1561 of the Affordable Care Act h. 45 CFR 164.316 and Administrative Rule 37.85.414

4. **Leverage Condition:** Tellus supports the open/hybrid EVV model and publishes standard open Application Program Interfaces (APIs) promoting interoperability across the Medicaid ecosystem by integrating with care management applications, third-party EVV vendors and MMIS.

5. **Business Rules Condition:** Tellus is passionate about understanding the perspectives of all EVV constituents. Our communications, outreach, training and customer support initiatives strive to promote a community of reliability, trust and respect. Our EVV solution supports accurate claims processing processes and procedures.

6. **Reporting Condition:** Tellus EVV collects and evaluates all the data necessary to evaluate the operation and performance of the EVV program to monitor and improve operations, transparency and accountability. AWS CloudWatch is used to monitor network traffic, bandwidth usage and bottlenecks that impede performance. Monitoring and auto-scaling systems provide the information required to diagnose system performance issues, errors and backlogs. Monitoring includes, but is not limited to, CPU, memory utilization, network and disk utilization. For the database server, we also monitor read/write latency, number of sessions and session performance. Our engineers get immediate notifications about all system issues. If these cannot be resolved immediately, notifications will be forwarded to the State and/or Providers as required based on service level agreements.

7. **Interoperability Condition:** Tellus uses Mirth Connect, an open source, cross-platform, bi-directional health care integration engine providing maximum flexibility to integrate with health information exchanges, public health agencies, human service programs and other community organizations as required.

To make sure we achieve certification objectives, we follow the CMS Medicaid Enterprise Certification Life Cycle (MECL) release and updated checklists, which include greater alignment to MITA, the Seven Conditions and Standards, and recent federal legislation. In 2017, CMS updated the MECL and Required Artifacts to include an Operational Milestone

Review (R2) before the operations go-live of the system, in addition to the traditional Certification Final Review (R3) at the end of the system stabilization period.

While final guidance around certification of EVV Systems by CMS has yet to be issued, Tellus agrees that in the future, the EVV System will need CMS certification. We will work cooperatively with the State to achieve this certification. CMS has not yet issued guidelines for EVV System certification; if CMS has still not issued certification guidelines and all other Phase 4 deliverables have been accepted, Tellus will invoice for those completed items and will invoice for the certification deliverable when certification has been achieved.

We align our efforts to ensure the delivered solution conforms to MITA 3.0 standards and with all of the required checklists items for modular certification, such as:

- Business Area Checklist
- General Checklists:
- Information Architecture Checklist
- Access and Delivery Checklist
- Integration and Utility Checklist
- Intermediary and Interface Checklist
- Standards and Conditions Checklist

Additionally, our technical and advisory teams are ready to support every phase of the certification process with the creation of the required documentation in the MECT V2.2, like:

- Project Management Plan
- Schedule/Milestones & Burn-down Charts
- Risk Register/Exception Plan
- Test Plan
- Working MMIS module(s) and software
- Earned Value/Velocity Management Report
- Database Design and DED
- Data Conversion/Management Plan
- Contingency/Recovery Plan
- Test Reports/Validated Product Reports
- System Design Document (SDD)
- System Requirement Document
- Product Documentation (User and Training Manuals)
- HIPAA Statemen

Tellus routinely monitors CMS communications and will remain in alignment with all future updates.

CMS recently published Medicaid Enterprise Certification Toolkit Version 2.3 (MECT v2.3) that applies to all MMIS and related state technology solutions excluding EVV. EVV requires a streamlined, outcomes-based approach to achieve certification. This approach focuses on demonstrating alignment with specific business outcomes. EVV certification is structured around the following elements:

- Pre Go-Live Operational Readiness Review
- Post Go-Live Certification Review (six months or more after Go-Live)
- Outcome statements
- Evaluation criteria and required evidence corresponding to outcome statements to evaluate the system's functionality and compliance with laws, regulations, and industry good practices
- Key performance indicators (KPIs) reported quarterly to support the outcome statements and track performance of the system over time

Tellus welcomes the opportunity to support DHHR in the new CMS outcomes-based certification process.

ATTACHMENT 10: MAINTENANCE AND OPERATIONS SPECIFICATIONS APPROACH

Instructions: Maintenance and Operations specifications ensure that the solution is fully functional and performing optimally until the end of the lifecycle. 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. 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).

OPERATIONS

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:
OP002	4716	2	The estimated and actual hours allocated to each change request
OP003	4717	2	Specific personnel assigned to each change request
OP004	4718	2	Scheduled completion date for each change request
OP005	4719	2	Total cost if the maximum allowed hours are exceeded on any approved change request
OP006	4720	2	Any change to current operational costs
OP007	4721	2	A separate total for equipment requirements (if applicable) related to the modification
OP008	5008	2	Others as defined by the Department

Tellus will track and provide DHHR access to process metrics and other detail as defined in the approved Change Management Plan. Information included in the plan will include:

- Estimated and actual hours allocated to each change request
- Specific personnel assigned to each change request

- Scheduled completion date for each change request
- Total cost if the maximum hours are exceeded on any approved change request
- Changes to current operational costs
- Equipment costs are not applicable
- Other information as requested by DHHR

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.

Tellus will review new patches of the software products as part of the routine maintenance process, and we will work with the DHHR on the application of patches for software and firmware within the solution. We first apply the patches to the non-production environment. After testing and sign-off, we apply them to the production environment.

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.

The Change Management Plan will include a policy related to software system updates will be defined and communicated to the project team. As a rule, our EVV application is updated on a quarterly basis with release notes shared with clients in advance so they are aware of enhancements, and we provide access to training materials if necessary.

If required due to changes in Federally mandated or National Standards compliance requirements (including but not limited to CMS, HIPAA, MITA) or technical issues, the application may be updated off cycle. All changes will be monitored through the documented change control process and communicated to constituents in a timely manner.

Tellus will inform the DHHR in advance of any scheduled maintenance. The following information will be communicated in advance for approval:

- Specific system functionality impacted by the maintenance, or modification/enhancement changed
- Planned implementation date
- Downtime, system unavailability, start and end time
- Communication plan to notify users and stakeholders
- A contingency plan in the event of implementation issues

Alerts will be pushed to the web-based consoles and via email in advance of any downtime so users are made aware and can plan accordingly. Scheduled maintenance will occur during off hours to ensure the least amount of impact.

OP011	4745	1	The Vendor should provide the Department with detailed documentation that provides all fixes and functionality for each release.

As a rule, our EVV application is updated on a quarterly basis with release notes shared with clients in advance so they are aware of enhancements, and we provide access to training materials if necessary.

System, portal and application updates will be released on an ongoing and as needed basis. Releases will maintain functionality, security and integrity of data. Releases that include new features and functionality may introduce additional configuration options for existing clients. Features and functions for upcoming releases will be communicated in advance of the release and existing clients will be educated about the options available as a result of the enhancements or modifications. They can adopt those changes by changing applicable business intelligence rules and configuration settings

OP012	4747	1	The Vendor should maintain version control and provide the Department with current system and user documentation.

Tellus provides ongoing training anytime a new release includes functionality or system changes that impact users. We also update training materials to coincide with the release and will make sure materials are updated prior to functionality or system changes. Materials will be accessible in electronic format for all users. All training materials will be provided to DHHR for review prior to initiating training sessions.

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.

Tellus will review new security patches of the software products as part of the routine maintenance process, and we will work with the DHHR on the application of security patches for software and firmware within the solution. We first apply the patches to the non-production environment. After testing and sign-off, we apply them to the production environment.

OP014	3960	1	The solution should provide the ability for the provider agency to review billing prior to submitting for payment.

Completed visits display on a Work List that is accessible from the web portal. There are three statuses for completed visits:

- New: New are newly completed visits that have not been through the Tellus pre-adjudication process which happens automatically based on rules set by your organization. These visits usually are completed daily. New visits/claims cannot be released until they have been through the Tellus pre-adjudication process, and when the process has been completed, the status of each visit will change to either Matched or Unmatched.
- Matched: Matched visits are ready to be released for payment. All information from the visit matches the prior authorization, service codes, recipient address and date and time of visit.
- Unmatched: Unmatched visits have errors or are missing information. A User with the appropriate role authorization can click a visit to view details of the visit and to see the errors and edits needed.

Users with the appropriate role-based authority can review all visits (including Matched) before they are submitted for payment.

OP015	5130	1	The solution should provide the ability for the provider agency to review and correct billing errors prior to submission.

All completed visits display on a Work List that is accessible from the web portal. Claims with the status Unmatched have errors or are missing information. Users with the appropriate role-based authority can drill down within any visit to see visit detail and to correct information as needed.

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:
OP017	5131	2	No authorization
OP018	5132	2	Expired authorization
OP019	5133	2	Reasons that prevented claims from filing
OP020	5134	2	Edits made to claims
OP021	5135	2	Others as defined by the Department

Reporting is available as defined, via both standard and ad hoc reporting capabilities. Visits completed without a valid authorization (missing or expired) and those missing elements required for matching are available (these missing elements would be a subset of the list of reasons that prevented claims from filing. Reports on edits made to visits can be made available as outlined in the requirements specifications document. Basically, any action and/or edits can be tracked and reported on by the Tellus system.

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:
OP023	5100	2	Browser-based

OP024	5101	2	Portable Document Format (PDF)
OP025	5102	2	Excel
OP026	5103	2	Comma-Separated Value (CSV)
OP027	5172	2	Others as defined by the Department

Contact Center reporting can be provided upon requested schedule and/or as needed, often as part of monthly standard reporting processes. Contacts may include calls, emails, web requests and/or chat.

OP028	4522	1	The solution should track metrics for each type of correspondence generated in the solution.

Inbound contacts may include calls, emails, web requests and/or chat, and volumes can be broken out by channel. All calls are recorded. Tracking is in place for emails, web requests and chat, and counts or other information is available upon request.

OP029	4526	1	The solution should track the status of notices that are moving through the generation process.

Contacts and their progress and resolution are tracked within a ZohoDesk ticketing system, and current status is always available (Open, Active, Resolved).

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.

Contact resolution timeframes are tracked, and delivery timeframes can be created and reminders can be sent and/or displayed as requested.

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.

Correspondence (client communication) is tracked when issued, reminders sent, or reissued/updated as requested.

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)

Tellus can provide annual statement on SOC audit as requested.

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.

Tellus can provide annual statement and action plan for remediation as requested.

OP034	4253	1	The solution should archive and store user profiles for a period of time agreed upon by the Department.

User profiles are archived and available upon request.

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.

Tellus has operationalized incident reporting and the associated policies and procedures. These documents are available for review and approval upon request.

OP036	4164	1	The Vendor should detail the performance metrics and targets used to monitor the effectiveness of technical support by phone.

Tellus gathers, reviews and monitors and can report on performance metrics and targets used to monitor the effectiveness of technical support by phone. Sample metrics include totally call volume (during and after business hours) Average Speed of Answer, Abandon Rate, Number of Calls that choose to leave a voice mail and other metrics as determined would be useful.

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.

Tellus utilizes a ZohoDesk ticketing system that is configured to provide an immediate response acknowledging the receipt of all email inquiries and that will include a ticket number for future reference, in addition to establishing a timeframe for the response.

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.

The Tellus Technical Support/Production Operations Team is available to troubleshoot email inquiries as requested, although for production-impacting issues email is not recommended. A status of production-impacting issues can be provided within 1 hour of request, and resolution is targeted within 4 hours of request. Should an issue need further escalation, customer will be provided ETA.

OP039	4167	1	The Vendor should document inquiries and provide the Department with routine reports regarding reasons for technical support requests.

Inquiries and other technical support requests and the resulting resolutions are tracked, and the following information is recorded in Zoho Service Desk:

- Initial complaint/inquiry
- Caller identification
- Date & time
- Message
- Steps taken to remediate
- Final resolution

Routine reports are available that classify inquiries as to the type received.

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.

Tellus is familiar with the importance of documenting procedural actions and improvements that occurred as a result of a complaint to the helpdesk. This information is available for submission to the Department on an agreed upon schedule.

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:
OP042	4928	2	Hours of operation
OP043	4929	2	Options for leaving messages after hours
OP044	4930	2	Options for leaving messages based on queue hold times and designated intervals as defined by the Department
OP045	4931	2	Recording of informational messages as defined by the Department

The help desk is accessed by a U.S.-based, toll-free telephone number that is operational 24/7/365. The number is connected to our help desk supported by English and Spanish speaking staff (and other languages upon request).

The interactive voice response system informs callers of the help desk hours of operation and provides them the option of leaving a message, both during and after normal business hours. Options for leaving messages are configurable based on queue hold times and/or designated intervals as defined by the Department.

Recording of informational messages as defined by the Department is also available upon request.

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:
OP047	5108	2	Average speed of answer
OP048	5109	2	Interface processing time
OP049	5110	2	Request time for report generation
OP050	5111	2	Others as defined by the Department

The Tellus Solution has the ability to record and report on the performance and utilization of resources within the overall system, including ASA, interface processing time, request time for ad hoc and standard report generation and others defined by the Department.

OP051	4500	1	The Vendor should document and maintain technical specifications associated with the solution including, but not limited to:
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.
OP053	4502	2	Complete specifications for all software, environments, and hardware used to support the solution.
OP054	4939	2	Others as defined by the Department

We will submit the technical documentation, including a final architectural diagram for each system environment, data dictionary, and high-level process flow diagram prior to contract signature. We will also negotiate the exact time frame for this delivery with DHHR prior to contract signature. DHHR will review and approve any architectural changes, relative to interface points with DHHR and external data sources before we implement them. We will implement integration point architecture changes in the lower environments first, and then promote them to upper environments after completing formal system integration testing (SIT) and user acceptance testing (UAT) and receiving DHHR approval.

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:
OP056	4940	2	Hardware
OP057	4941	2	Environment
OP058	4942	2	Network specifications
OP059	5106	2	Others as defined by the Department

Because our solution is cloud hosted and accessed using personal computers, smart devices and operating systems, there are no limitations to the number of concurrent users who can access the application. The application is highly scalable with additional capacity managed by adding virtual machines as required to make sure performance standards are not compromised.

OP060	4661	1	The solution should provide real-time solution performance data.

Tellus monitors all components of the EVV platform real time using automated tools. Our infrastructure team is alerted immediately if any performance metrics are reporting abnormal results.

OP061	4663	1	The solution should report on total processing times based on user-defined queries.

Tellus monitors processing times using automated tools that monitor application performance.

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.

Tellus EVV retains audit logs including exception reports and error logs. Tellus can make these available to DHHR in a standard format for review upon request.

OP063	4740	1	The solution should allow the Department's administrator to view, filter, sort, and search the error log(s).

Tellus EVV retains audit logs including exception reports and error logs. Tellus can make these available to DHHR in a standard that will provide the DHHR administrator with the ability to view, filter, sort and search the logs.

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.

Tellus will notify DHHR if any releases of third-party software are known to create problems with the current version of our software.

OP065	4773	1	The solution should schedule and support file transfers as requested and agreed upon by the Department.

Data interchange may be in asynchronous batch mode or synchronous transactional mode. The general sequence of events is the same for synchronous or asynchronous, with the difference being in the timing of imports, exports and response messages, as defined by DHHR

OP066	3946	1	The solution's data aggregation component should send each provider agency a verified visit report, at least once a calendar day.

The Tellus solution updates in near-real-time, so a provider agency can view a verified visit report through our Administrative Console/Dashboard at any time.

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.

The Tellus solution updates in near-real-time, so a provider agency can view a visit not verified visit report through our Administrative Console/Dashboard at any time.

Solution Backup, Disaster Recovery, and Failover

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.

The database is a critical component of the system. We use Amazon RDS (Relational Database Service) to host our database server. Amazon RDS runs on the same highly reliable infrastructure used by other Amazon Web Services. In production, we provision Multi-AZ database instances.

Amazon RDS synchronously replicates the data to a standby instance in a different Availability Zone (different datacenter). In case of failure of the primary node, Amazon RDS performs an automatic failover to the standby without the need for manual administrative intervention. When a failover is performed, there is a very short period during which the primary node is not accessible. We use many Amazon RDS features that enhance reliability for critical production databases, including automated backups, database snapshots, and automatic host replacement in case of primary database crash. In addition to synchronous replication, database backup snapshots are taken at regular intervals and sent to AWS S3 encrypted storage

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.

Amazon RDS runs on the same highly reliable infrastructure and synchronously replicates the data to a standby instance in a different Availability Zone (different datacenter). RDS features we use to enhance reliability for critical production databases include: automated backups, database snapshots, and automatic host replacement in case of primary database crash. Database backup snapshots are taken at regular intervals and sent to AWS S3 encrypted storage

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.

Tellus EVV performs back-ups during non-peak processing hours. The solution can continue to be used during back-ups.

DR004	4331	1	The solution should support data freezing.

Tellus requires additional information regarding this requirement.

DR005	4261	1	The Vendor should maintain an operational back-up power supply capable of supporting vital functions.

Tellus EVV uses the AWS Government Cloud and runs on fifteen (15) AWS datacenters located in the continental U.S. AWS datacenters are distributed in geographic regions which include clusters of datacenters called Availability Zones. Every region is geographically isolated in terms of power and water supply, and each zone is similarly served by independent networks. Redundantly storing information in different datacenters in multiple regions, availability zones, and datacenters greatly reduces downtime, as the nearest availability zone is activated as a backup when necessary.

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.

Each AWS datacenter is protected by distinct layers of security safeguarding both data and equipment. A layering approach to security helps ensure that failure of one element in the system doesn't create vulnerability in the whole system The Infrastructure Layer comprises energy generators, fire suppression equipment, and ordinary and extraordinary maintenance systems to protect the integrity of the data stored in the datacenter. An Environmental Layer at the locations where AWS datacenters are built are screened for seismic activity and extreme weather, to minimize the risk of structural damage caused by natural occurrences.

DR007	4291	1	The Vendor should equip fire detection and alarm systems with uninterruptable power supply.

Tellus EVV is hosted on AWS cloud.

DR008	4293	1	The Vendor should have a remote backup facility at least one hundred (100) miles away from the primary data center.

The EVV platform is hosted on Amazon Web Services (AWS) Government Cloud and runs on 15 AWS data centers located in the continental U.S. AWS datacenters are distributed in geographic regions that include clusters of datacenters called Availability Zones. Every region is geographically isolated in terms of power and water supply, and each zone is similarly served by independent networks. Redundantly storing information in different datacenters in multiple regions, availability zones and datacenters greatly reduces downtime, as the nearest available node is activated as a backup

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.

Tellus will provide a comprehensive Disaster Recovery and Business Continuity Plan (DR Plan) for this project. The DR Plan will be updated at least annually or any time a major system update or upgrade is performed. The Disaster Recovery Lead will be responsible for updating the entire document and permitted to request information and updates from other employees and departments within the organization to complete this task.

The DR Plan limits service interruptions to a period of 24 hours. However, because our systems are fully utilizing scalability, disaster recovery, high availability and monitoring features of AWS, we do not anticipate that recovery time will be anywhere near 24 hours.

The comprehensive DR Plan will be provided to the Agency when it's modified, or at least

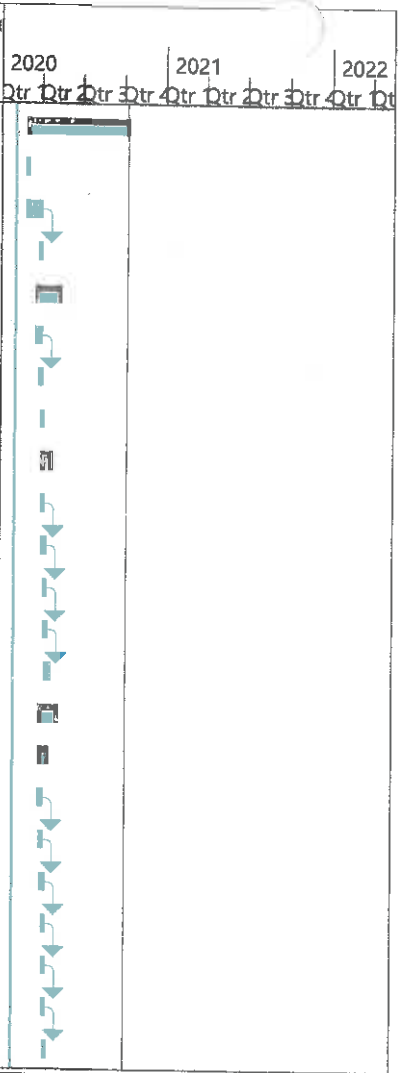
annually, as a PDF file. At the DHHR's request, in accordance to the best interests of the DHHR, the DR Plan will be updated at no additional cost.

The DR Plan will be tested annually or after major infrastructure or system changes to ensure completeness and effectiveness of the existing DR Plan. Results of the testing will be submitted as soon as the test is complete — and at least annually.

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.

All backups and recovery of databases for all cases, including disaster and system failure, are hosted in at least two different availability zones (geographically different data centers). Database instances are kept in sync real-time. Backups are scheduled and occur at regular intervals. They are then encrypted and stored in multiple locations providing 99.9% durability.

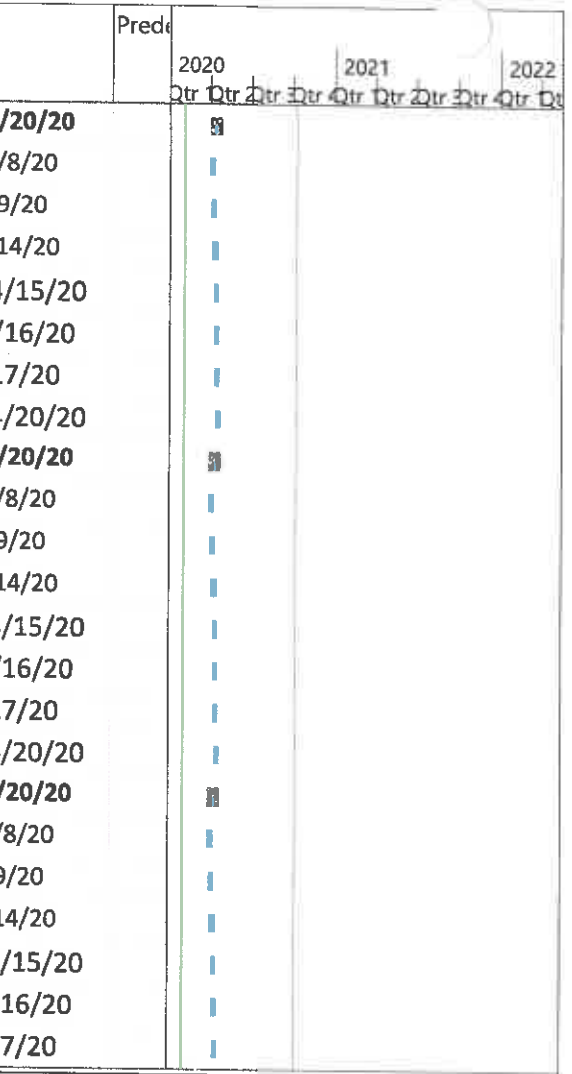
ID	Task N	Du	Start	Finish	Prede
1	**West Virginia Draft Project Schedule**	**158 days?**	**Mon 3/2/20**	**Wed 10/7/20**	
2	Contract Award Made	1 day	Mon 3/2/20	Mon 3/2/20	
3	Contract Negotiations/Review Period	20 days	Wed 3/4/20	Tue 3/31/20	
4	Contract Execution	1 day	Wed 4/1/20	Wed 4/1/20	3
5	**Task Group 1 - Project Initiation and Planning Phase**	**34 days?**	**Wed 3/25/20**	**Mon 5/11/20**	
6	Tellus Creates Project Kick-off Materials	6 days	Wed 3/25/20	Wed 4/1/20	
7	Deliver Project Kick-off Materials to DHHR	1 day	Thu 4/2/20	Thu 4/2/20	6
8	Project Kick-off Meeting	1 day	Mon 4/6/20	Mon 4/6/20	
9	**Annoucement Letter**	**12 days**	**Wed 4/8/20**	**Thu 4/23/20**	
10	Draft Delivered to DHHR	1 day	Wed 4/8/20	Wed 4/8/20	
11	DHHR Review Announcement Letter	3 days	Thu 4/9/20	Mon 4/13/20	10
12	Announcment Letter Revisions	1 day	Tue 4/14/20	Tue 4/14/20	11
13	Announcment Letter Approval	2 days	Wed 4/15/20	Thu 4/16/20	12
14	Delivery/Distribution of Announcment Letter	5 days	Fri 4/17/20	Thu 4/23/20	13
15	**Project Management Plan**	**26 days?**	**Mon 4/6/20**	**Mon 5/11/20**	
16	**Change Management Plan**	**11 days**	**Mon 4/6/20**	**Mon 4/20/20**	
17	Draft Created by Tellus	3 days	Mon 4/6/20	Wed 4/8/20	
18	Draft Delivered to DHHR	1 day	Thu 4/9/20	Thu 4/9/20	17
19	Draft Reviewed by DHHR	3 days	Fri 4/10/20	Tue 4/14/20	18
20	Marks/Comments Returned by DHHR	1 day	Wed 4/15/20	Wed 4/15/20	19
21	Plan Revisions By Tellus	1 day	Thu 4/16/20	Thu 4/16/20	20
22	Revised Version Delivered to DHHR	1 day	Fri 4/17/20	Fri 4/17/20	21
23	DHHR Approval of Final Plan	1 day	Mon 4/20/20	Mon 4/20/20	22



Project: West Virginia Project
Plan Date: Wed 2/5/2020

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

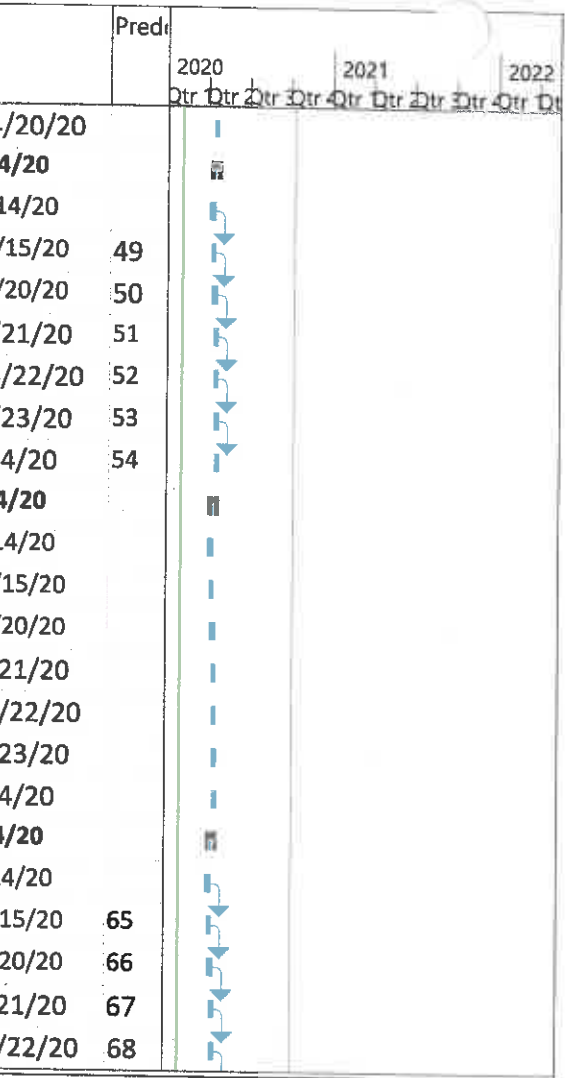
ID	Task N	Du	Start	Finish	Prede
24	**Communication Plan**	**11 days**	**Mon 4/6/20**	**Mon 4/20/20**	
25	Draft Created by Tellus	3 days	Mon 4/6/20	Wed 4/8/20	
26	Draft Delivered to DHHR	1 day	Thu 4/9/20	Thu 4/9/20	
27	Draft Reviewed by DHHR	3 days	Fri 4/10/20	Tue 4/14/20	
28	Marks/Comments Returned by DHHR	1 day	Wed 4/15/20	Wed 4/15/20	
29	Plan Revisions By Tellus	1 day	Thu 4/16/20	Thu 4/16/20	
30	Revised Version Delivered to DHHR	1 day	Fri 4/17/20	Fri 4/17/20	
31	DHHR Approval of Final Plan	1 day	Mon 4/20/20	Mon 4/20/20	
32	**Cost Management Plan**	**11 days**	**Mon 4/6/20**	**Mon 4/20/20**	
33	Draft Created by Tellus	3 days	Mon 4/6/20	Wed 4/8/20	
34	Draft Delivered to DHHR	1 day	Thu 4/9/20	Thu 4/9/20	
35	Draft Reviewed by DHHR	3 days	Fri 4/10/20	Tue 4/14/20	
36	Marks/Comments Returned by DHHR	1 day	Wed 4/15/20	Wed 4/15/20	
37	Plan Revisions By Tellus	1 day	Thu 4/16/20	Thu 4/16/20	
38	Revised Version Delivered to DHHR	1 day	Fri 4/17/20	Fri 4/17/20	
39	DHHR Approval of Final Plan	1 day	Mon 4/20/20	Mon 4/20/20	
40	**Documentation Management Plan**	**11 days**	**Mon 4/6/20**	**Mon 4/20/20**	
41	Draft Created by Tellus	3 days	Mon 4/6/20	Wed 4/8/20	
42	Draft Delivered to DHHR	1 day	Thu 4/9/20	Thu 4/9/20	
43	Draft Reviewed by DHHR	3 days	Fri 4/10/20	Tue 4/14/20	
44	Marks/Comments Returned by DHHR	1 day	Wed 4/15/20	Wed 4/15/20	
45	Plan Revisions By Tellus	1 day	Thu 4/16/20	Thu 4/16/20	
46	Revised Version Delivered to DHHR	1 day	Fri 4/17/20	Fri 4/17/20	



Project: West Virginia Project
Plan Date: Wed 2/5/20

Task	Inactive Summary	External Tasks
Split	Manual Task	External Milestone
Milestone	Duration-only	Deadline
Summary	Manual Summary Rollup	Progress
Project Summary	Manual Summary	Manual Progress
Inactive Task	Start-only	
Inactive Milestone	Finish-only	

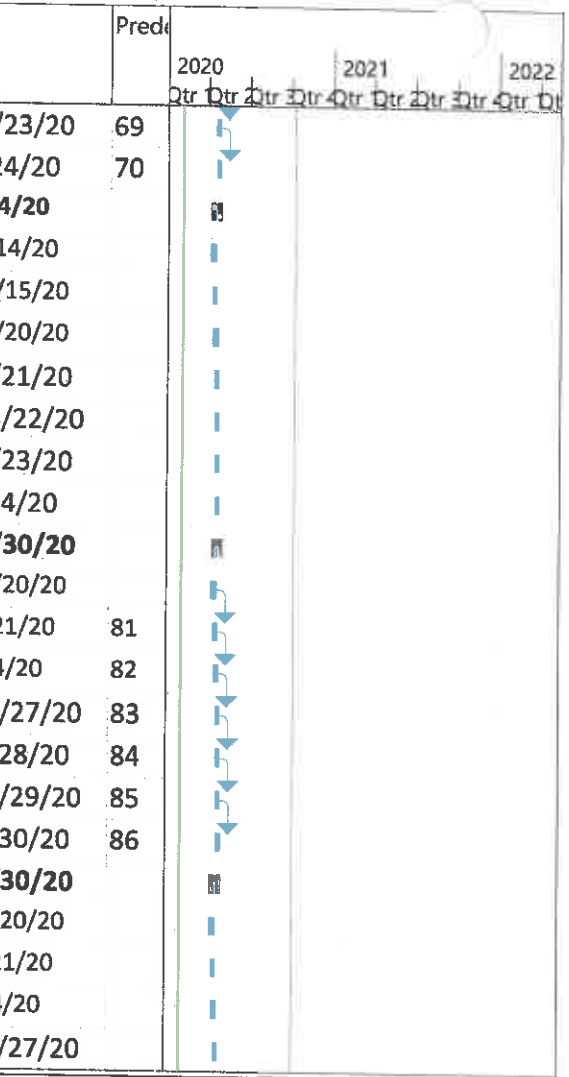
ID	Task Name	Duration	Start	Finish	Predecessors
47	DHHR Approval of Final Plan	1 day	Mon 4/20/20	Mon 4/20/20	
48	**Modularity and Reusability Plan**	**11 days**	**Fri 4/10/20**	**Fri 4/24/20**	
49	Draft Created by Tellus	3 days	Fri 4/10/20	Tue 4/14/20	
50	Draft Delivered to DHHR	1 day	Wed 4/15/20	Wed 4/15/20	49
51	Draft Reviewed by DHHR	3 days	Thu 4/16/20	Mon 4/20/20	50
52	Marks/Comments Returned by DHHR	1 day	Tue 4/21/20	Tue 4/21/20	51
53	Plan Revisions By Tellus	1 day	Wed 4/22/20	Wed 4/22/20	52
54	Revised Version Delivered to DHHR	1 day	Thu 4/23/20	Thu 4/23/20	53
55	DHHR Approval of Final Plan	1 day	Fri 4/24/20	Fri 4/24/20	54
56	**Project Work Plan**	**11 days**	**Fri 4/10/20**	**Fri 4/24/20**	
57	Draft Created by Tellus	3 days	Fri 4/10/20	Tue 4/14/20	
58	Draft Delivered to DHHR	1 day	Wed 4/15/20	Wed 4/15/20	
59	Draft Reviewed by DHHR	3 days	Thu 4/16/20	Mon 4/20/20	
60	Marks/Comments Returned by DHHR	1 day	Tue 4/21/20	Tue 4/21/20	
61	Plan Revisions By Tellus	1 day	Wed 4/22/20	Wed 4/22/20	
62	Revised Version Delivered to DHHR	1 day	Thu 4/23/20	Thu 4/23/20	
63	DHHR Approval of Final Plan	1 day	Fri 4/24/20	Fri 4/24/20	
64	**Quality Management Plan**	**11 days**	**Fri 4/10/20**	**Fri 4/24/20**	
65	Draft Created by Tellus	3 days	Fri 4/10/20	Tue 4/14/20	
66	Draft Delivered to DHHR	1 day	Wed 4/15/20	Wed 4/15/20	65
67	Draft Reviewed by DHHR	3 days	Thu 4/16/20	Mon 4/20/20	66
68	Marks/Comments Returned by DHHR	1 day	Tue 4/21/20	Tue 4/21/20	67
69	Plan Revisions By Tellus	1 day	Wed 4/22/20	Wed 4/22/20	68



Project: West Virginia Project
Plan Date: Wed 2/5/20

Task	Inactive Summary	External Tasks
Split	Manual Task	External Milestone
Milestone	Duration-only	Deadline
Summary	Manual Summary Rollup	Progress
Project Summary	Manual Summary	Manual Progress
Inactive Task	Start-only	
Inactive Milestone	Finish-only	

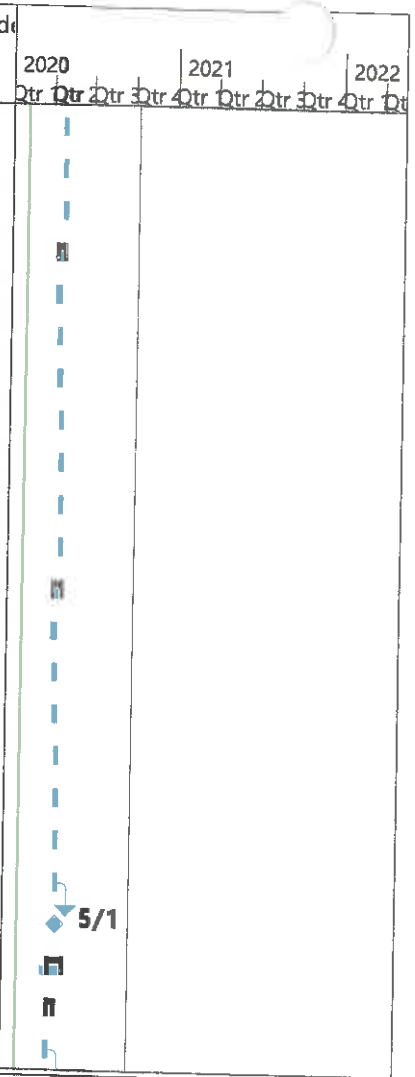
ID	Task N	Du	Start	Finish	Prede
70	Revised Version Delivered to DHHR	1 day	Thu 4/23/20	Thu 4/23/20	69
71	DHHR Approval of Final Plan	1 day	Fri 4/24/20	Fri 4/24/20	70
72	**Risk and Issues Management Plan**	**11 days**	**Fri 4/10/20**	**Fri 4/24/20**	
73	Draft Created by Tellus	3 days	Fri 4/10/20	Tue 4/14/20	
74	Draft Delivered to DHHR	1 day	Wed 4/15/20	Wed 4/15/20	
75	Draft Reviewed by DHHR	3 days	Thu 4/16/20	Mon 4/20/20	
76	Marks/Comments Returned by DHHR	1 day	Tue 4/21/20	Tue 4/21/20	
77	Plan Revisions By Tellus	1 day	Wed 4/22/20	Wed 4/22/20	
78	Revised Version Delivered to DHHR	1 day	Thu 4/23/20	Thu 4/23/20	
79	DHHR Approval of Final Plan	1 day	Fri 4/24/20	Fri 4/24/20	
80	**Schedule Management Plan**	**11 days**	**Thu 4/16/20**	**Thu 4/30/20**	
81	Draft Created by Tellus	3 days	Thu 4/16/20	Mon 4/20/20	
82	Draft Delivered to DHHR	1 day	Tue 4/21/20	Tue 4/21/20	81
83	Draft Reviewed by DHHR	3 days	Wed 4/22/20	Fri 4/24/20	82
84	Marks/Comments Returned by DHHR	1 day	Mon 4/27/20	Mon 4/27/20	83
85	Plan Revisions By Tellus	1 day	Tue 4/28/20	Tue 4/28/20	84
86	Revised Version Delivered to DHHR	1 day	Wed 4/29/20	Wed 4/29/20	85
87	DHHR Approval of Final Plan	1 day	Thu 4/30/20	Thu 4/30/20	86
88	**Scope Management Plan**	**11 days**	**Thu 4/16/20**	**Thu 4/30/20**	
89	Draft Created by Tellus	3 days	Thu 4/16/20	Mon 4/20/20	
90	Draft Delivered to DHHR	1 day	Tue 4/21/20	Tue 4/21/20	
91	Draft Reviewed by DHHR	3 days	Wed 4/22/20	Fri 4/24/20	
92	Marks/Comments Returned by DHHR	1 day	Mon 4/27/20	Mon 4/27/20	



Project: West Virginia Project
Plan Date: Wed 2/5/20

Task	Inactive Summary	External Tasks
Split	Manual Task	External Milestone
Milestone	Duration-only	Deadline
Summary	Manual Summary Rollup	Progress
Project Summary	Manual Summary	Manual Progress
Inactive Task	Start-only	
Inactive Milestone	Finish-only	

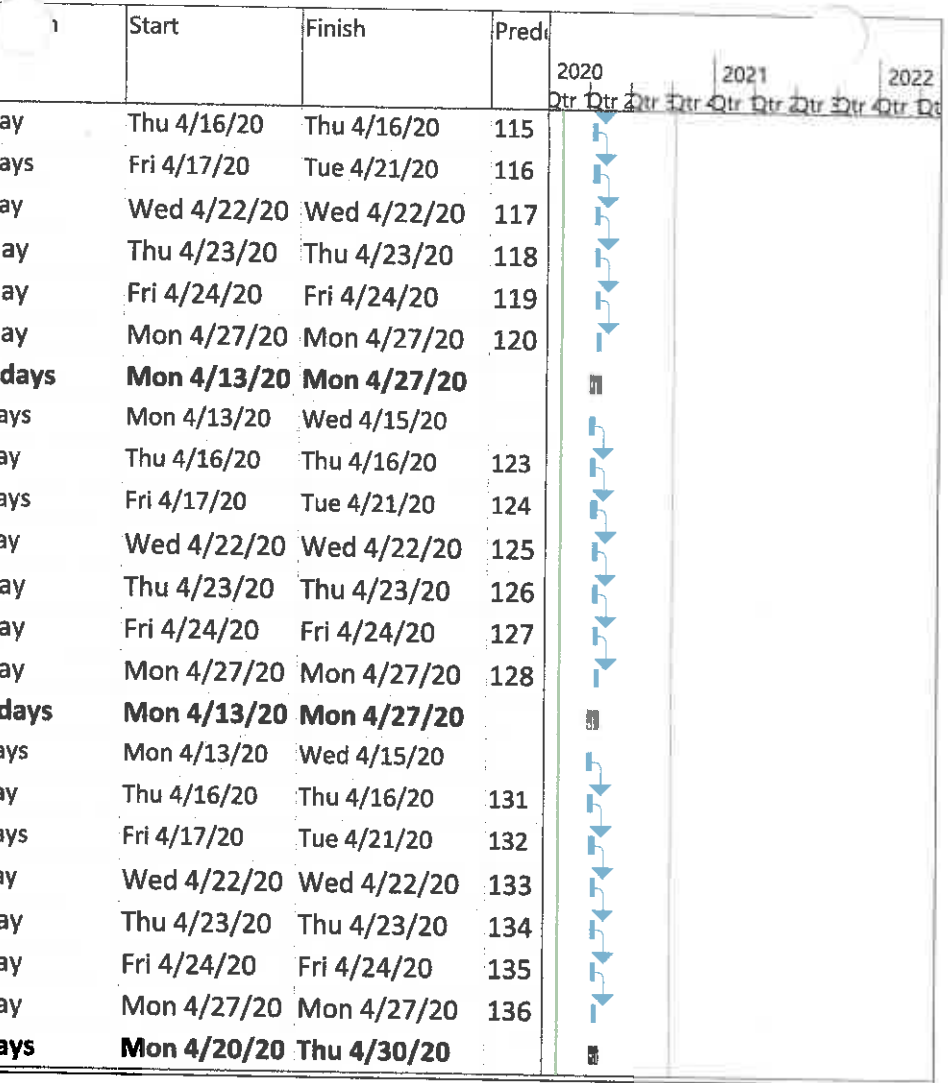
ID	Task N	Du	Start	Finish	Prede
93	Plan Revisions By Tellus	1 day	Tue 4/28/20	Tue 4/28/20	
94	Revised Version Delivered to DHHR	1 day	Wed 4/29/20	Wed 4/29/20	
95	DHHR Approval of Final Plan	1 day	Thu 4/30/20	Thu 4/30/20	
96	**Staffing Management Plan**	**11 days**	**Thu 4/16/20**	**Thu 4/30/20**	
97	Draft Created by Tellus	3 days	Thu 4/16/20	Mon 4/20/20	
98	Draft Delivered to DHHR	1 day	Tue 4/21/20	Tue 4/21/20	
99	Draft Reviewed by DHHR	3 days	Wed 4/22/20	Fri 4/24/20	
100	Marks/Comments Returned by DHHR	1 day	Mon 4/27/20	Mon 4/27/20	
101	Plan Revisions By Tellus	1 day	Tue 4/28/20	Tue 4/28/20	
102	Revised Version Delivered to DHHR	1 day	Wed 4/29/20	Wed 4/29/20	
103	DHHR Approval of Final Plan	1 day	Thu 4/30/20	Thu 4/30/20	
104	**Stakeholder Management Plan and Stakeholder Analysis**	**12 days**	**Thu 4/16/20**	**Fri 5/1/20**	
105	Draft Created by Tellus	3 days	Thu 4/16/20	Mon 4/20/20	
106	Draft Delivered to DHHR	1 day	Tue 4/21/20	Tue 4/21/20	
107	Draft Reviewed by DHHR	3 days	Wed 4/22/20	Fri 4/24/20	
108	Marks/Comments Returned by DHHR	1 day	Mon 4/27/20	Mon 4/27/20	
109	Plan Revisions By Tellus	1 day	Tue 4/28/20	Tue 4/28/20	
110	Revised Version Delivered to DHHR	1 day	Wed 4/29/20	Wed 4/29/20	
111	DHHR Approval of Final Plan	1 day	Thu 4/30/20	Thu 4/30/20	
112	*Milestone 1 - Project Initiation Phase Complete*	*0 days*	*Fri 5/1/20*	*Fri 5/1/20*	*111*
113	**Task Group 2 - Solution Planning Phase**	**24 days?**	**Mon 4/13/20**	**Thu 5/14/20**	
114	**Data Management Plan**	**11 days**	**Mon 4/13/20**	**Mon 4/27/20**	
115	Draft Created by Tellus	3 days	Mon 4/13/20	Wed 4/15/20	



Project: West Virginia Project
Plan Date: Wed 2/5/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

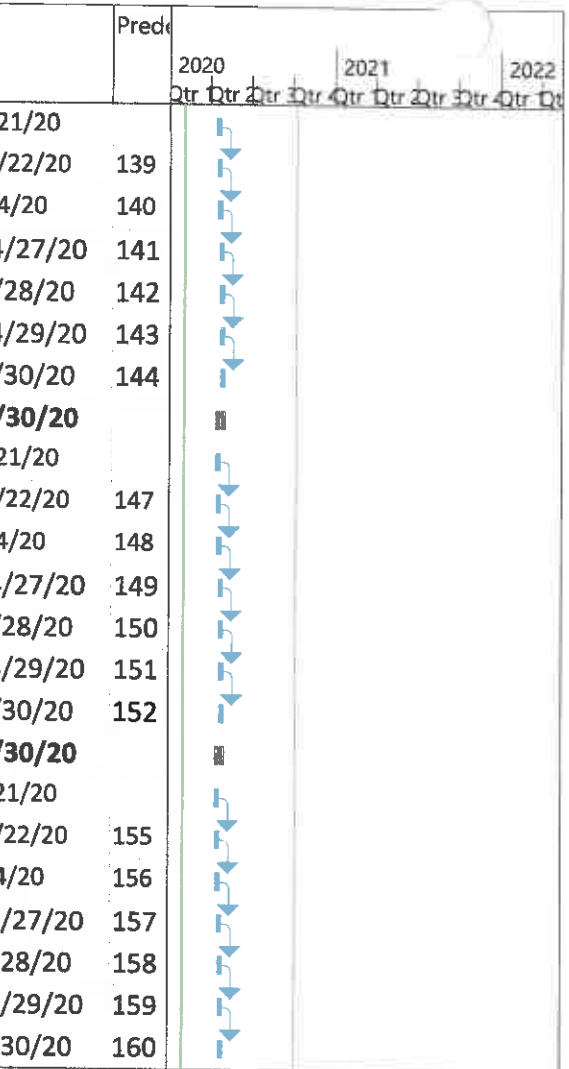
ID	Task N	Du	Start	Finish	Pred
116	Draft Delivered to DHHR	1 day	Thu 4/16/20	Thu 4/16/20	115
117	Draft Reviewed by DHHR	3 days	Fri 4/17/20	Tue 4/21/20	116
118	Marks/Comments Returned by DHHR	1 day	Wed 4/22/20	Wed 4/22/20	117
119	Plan Revisions By Tellus	1 day	Thu 4/23/20	Thu 4/23/20	118
120	Revised Version Delivered to DHHR	1 day	Fri 4/24/20	Fri 4/24/20	119
121	DHHR Approval of Final Plan	1 day	Mon 4/27/20	Mon 4/27/20	120
122	**Data Security, Privacy, and Confidentiality Plan**	**11 days**	**Mon 4/13/20**	**Mon 4/27/20**	
123	Draft Created by Tellus	3 days	Mon 4/13/20	Wed 4/15/20	
124	Draft Delivered to DHHR	1 day	Thu 4/16/20	Thu 4/16/20	123
125	Draft Reviewed by DHHR	3 days	Fri 4/17/20	Tue 4/21/20	124
126	Marks/Comments Returned by DHHR	1 day	Wed 4/22/20	Wed 4/22/20	125
127	Plan Revisions By Tellus	1 day	Thu 4/23/20	Thu 4/23/20	126
128	Revised Version Delivered to DHHR	1 day	Fri 4/24/20	Fri 4/24/20	127
129	DHHR Approval of Final Plan	1 day	Mon 4/27/20	Mon 4/27/20	128
130	**Incident Management Plan**	**11 days**	**Mon 4/13/20**	**Mon 4/27/20**	
131	Draft Created by Tellus	3 days	Mon 4/13/20	Wed 4/15/20	
132	Draft Delivered to DHHR	1 day	Thu 4/16/20	Thu 4/16/20	131
133	Draft Reviewed by DHHR	3 days	Fri 4/17/20	Tue 4/21/20	132
134	Marks/Comments Returned by DHHR	1 day	Wed 4/22/20	Wed 4/22/20	133
135	Plan Revisions By Tellus	1 day	Thu 4/23/20	Thu 4/23/20	134
136	Revised Version Delivered to DHHR	1 day	Fri 4/24/20	Fri 4/24/20	135
137	DHHR Approval of Final Plan	1 day	Mon 4/27/20	Mon 4/27/20	136
138	**Privacy Impact Analysis**	**9 days**	**Mon 4/20/20**	**Thu 4/30/20**	



Project: West Virginia Project
Plan Date: Wed 2/5/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

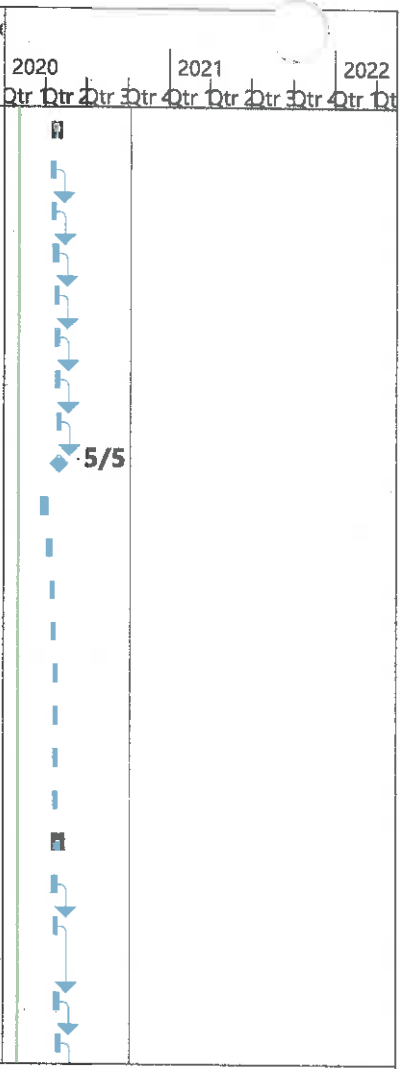
ID	Task N	Du	Start	Finish	Prede
139	Draft Created by Tellus	2 days	Mon 4/20/20	Tue 4/21/20	
140	Draft Delivered to DHHR	1 day	Wed 4/22/20	Wed 4/22/20	139
141	Draft Reviewed by DHHR	2 days	Thu 4/23/20	Fri 4/24/20	140
142	Marks/Comments Returned by DHHR	1 day	Mon 4/27/20	Mon 4/27/20	141
143	Plan Revisions By Tellus	1 day	Tue 4/28/20	Tue 4/28/20	142
144	Revised Version Delivered to DHHR	1 day	Wed 4/29/20	Wed 4/29/20	143
145	DHHR Approval of Final Plan	1 day	Thu 4/30/20	Thu 4/30/20	144
146	**Requirements Gap Analysis Document**	**9 days**	**Mon 4/20/20**	**Thu 4/30/20**	
147	Draft Created by Tellus	2 days	Mon 4/20/20	Tue 4/21/20	
148	Draft Delivered to DHHR	1 day	Wed 4/22/20	Wed 4/22/20	147
149	Draft Reviewed by DHHR	2 days	Thu 4/23/20	Fri 4/24/20	148
150	Marks/Comments Returned by DHHR	1 day	Mon 4/27/20	Mon 4/27/20	149
151	Plan Revisions By Tellus	1 day	Tue 4/28/20	Tue 4/28/20	150
152	Revised Version Delivered to DHHR	1 day	Wed 4/29/20	Wed 4/29/20	151
153	DHHR Approval of Final Plan	1 day	Thu 4/30/20	Thu 4/30/20	152
154	**Requirements Management Plan**	**9 days**	**Mon 4/20/20**	**Thu 4/30/20**	
155	Draft Created by Tellus	2 days	Mon 4/20/20	Tue 4/21/20	
156	Draft Delivered to DHHR	1 day	Wed 4/22/20	Wed 4/22/20	155
157	Draft Reviewed by DHHR	2 days	Thu 4/23/20	Fri 4/24/20	156
158	Marks/Comments Returned by DHHR	1 day	Mon 4/27/20	Mon 4/27/20	157
159	Plan Revisions By Tellus	1 day	Tue 4/28/20	Tue 4/28/20	158
160	Revised Version Delivered to DHHR	1 day	Wed 4/29/20	Wed 4/29/20	159
161	DHHR Approval of Final Plan	1 day	Thu 4/30/20	Thu 4/30/20	160



Project: West Virginia Project
Plan Date: Wed 2/5/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

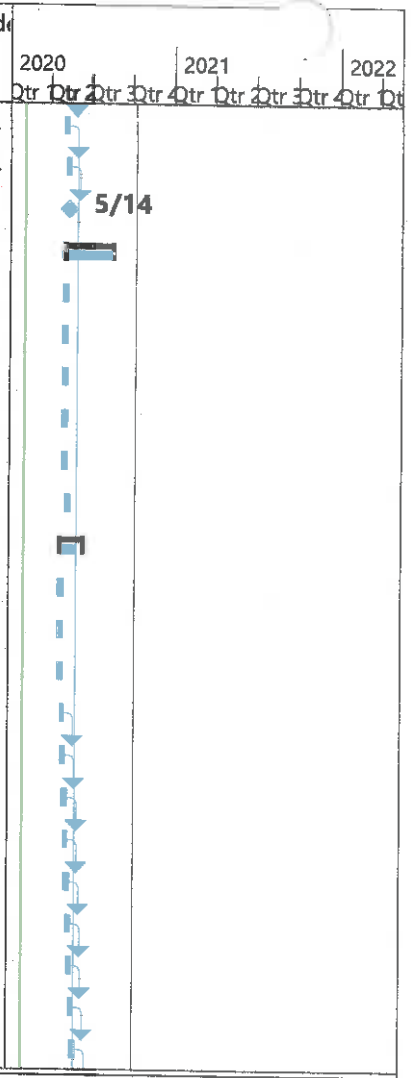
ID	Task Name	Duration	Start	Finish	Predecessors
162	**Master Test Plan (Testing Management Plan)**	**11 days**	**Mon 4/20/20**	**Mon 5/4/20**	
163	Draft Created by Tellus	3 days	Mon 4/20/20	Wed 4/22/20	
164	Draft Delivered to DHHR	1 day	Thu 4/23/20	Thu 4/23/20	163
165	Draft Reviewed by DHHR	3 days	Fri 4/24/20	Tue 4/28/20	164
166	Marks/Comments Returned by DHHR	1 day	Wed 4/29/20	Wed 4/29/20	165
167	Plan Revisions By Tellus	1 day	Thu 4/30/20	Thu 4/30/20	166
168	Revised Version Delivered to DHHR	1 day	Fri 5/1/20	Fri 5/1/20	167
169	DHHR Approval of Final Plan	1 day	Mon 5/4/20	Mon 5/4/20	168
170	*Milestone 2 - Solution Planning 1 Complete*	*0 days*	*Tue 5/5/20*	*Tue 5/5/20*	*169*
171	Secure Training Locations	7 days	Mon 3/30/20	Tue 4/7/20	
172	Joint Application Development (JAD) session 1 (on-site)	4 days	Mon 4/13/20	Thu 4/16/20	
173	Joint Application Development (JAD) session 2 (virtual)	1 day	Tue 4/21/20	Tue 4/21/20	
174	Joint Application Development (JAD) session 3 (virtual)	1 day	Thu 4/23/20	Thu 4/23/20	
175	Requirements Traceability Matrix Delivered to DHHR	1 day	Tue 4/28/20	Tue 4/28/20	
176	Safeguard Procedure Report Delivered to DHHR	1 day	Tue 4/28/20	Tue 4/28/20	
177	Security Plan	1 day	Tue 4/28/20	Tue 4/28/20	
178	System Backup and Record Retention Plan	1 day	Tue 4/28/20	Tue 4/28/20	
179	**Requirements Specification Document**	**15 days**	**Fri 4/24/20**	**Thu 5/14/20**	
180	Requirements Specification Document Draft	3 days	Fri 4/24/20	Tue 4/28/20	
181	Requirements Specification Document Delivered to DHHR for Review	1 day	Wed 4/29/20	Wed 4/29/20	180
182	Marks/Comments Returned by DHHR for RSD	3 days	Thu 4/30/20	Mon 5/4/20	181
183	Tellus Revision of RSD	2 days	Tue 5/5/20	Wed 5/6/20	182



Project: West Virginia Project
Plan Date: Wed 2/5/20

Task	Inactive Summary	External Tasks
Split	Manual Task	External Milestone
Milestone	Duration-only	Deadline
Summary	Manual Summary Rollup	Progress
Project Summary	Manual Summary	Manual Progress
Inactive Task	Start-only	
Inactive Milestone	Finish-only	

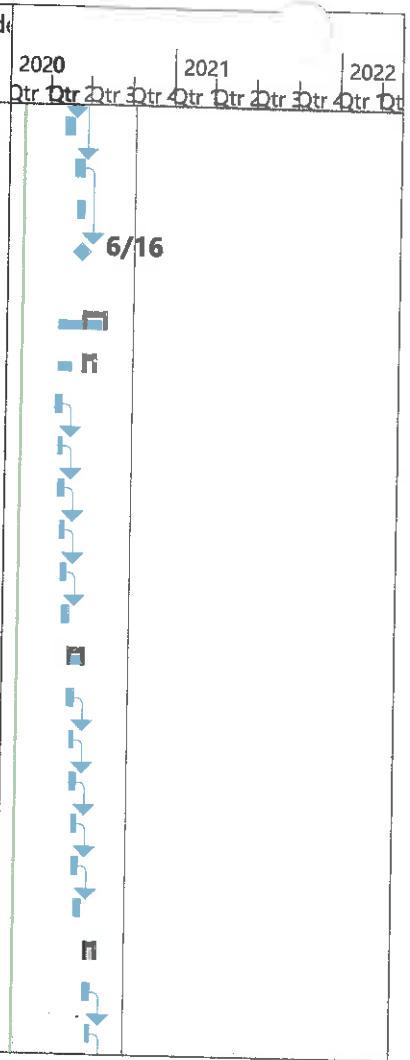
ID	Task N	Du	Start	Finish	Prede
184	DHHR Approval/Sign-off of Requirements Specifications Docum	2 days	Thu 5/7/20	Fri 5/8/20	183
185	System Requirement Document/Backlog User Stories or Use Case	3 days	Mon 5/11/20	Wed 5/13/20	184
186	*Milestone 3 - Solution Planning 2 Complete*	*0 days*	*Thu 5/14/20*	*Thu 5/14/20*	*185*
187	**Task Group 3 - Solution Design, Testing, and Operational Readiness**	**78 days**	**Mon 5/4/20**	**Wed 8/19/20**	
188	Diaster Recovery and Business Continuity Plan	5 days	Mon 5/4/20	Fri 5/8/20	
189	Database Design Document and Data Models	5 days	Mon 5/4/20	Fri 5/8/20	
190	Detailed System Design Document	5 days	Mon 5/4/20	Fri 5/8/20	
191	Capacity Plan	5 days	Mon 5/4/20	Fri 5/8/20	
192	Configuration Management Plan	5 days	Mon 5/4/20	Fri 5/8/20	
193	Data Conversion Plan	5 days	Mon 5/11/20	Fri 5/15/20	
194	**Integration Tasks**	**37 days**	Mon 4/27/20	Tue 6/16/20	
195	SFTP Setup	5 days	Mon 4/27/20	Fri 5/1/20	
196	Channel Configuration	5 days	Mon 4/27/20	Fri 5/1/20	
197	Database Setup	5 days	Mon 4/27/20	Fri 5/1/20	
198	PA, Member, Provider Sample File Deliveried to Tellus - Cycle 1	1 day	Mon 5/4/20	Mon 5/4/20	
199	PA, Member, Provider Sample File Results to DHHR - Cycle 1	3 days	Tue 5/5/20	Thu 5/7/20	198
200	PA, Member, Provider File Updates/Corrections - Cycle 1	3 days	Fri 5/8/20	Tue 5/12/20	199
201	PA, Member, Provider Sample File Deliveried to Tellus - Cycle 2	1 day	Wed 5/13/20	Wed 5/13/20	200
202	PA, Member, Provider Sample File Results to DHHR - Cycle 2	3 days	Thu 5/14/20	Mon 5/18/20	201
203	PA, Member, Provider File Updates/Corrections - Cycle 2	3 days	Tue 5/19/20	Thu 5/21/20	202
204	PA, Member, Provider Sample File Deliveried to Tellus - Cycle 3	1 day	Fri 5/22/20	Fri 5/22/20	203
205	PA, Member, Provider Sample File Results to DHHR - Cycle 3	3 days	Mon 5/25/20	Wed 5/27/20	204
206	PA, Member, Provider File Updates/Corrections - Cycle 3	3 days	Thu 5/28/20	Mon 6/1/20	205



Project: West Virginia Project
Plan Date: Wed 2/5/20

Task	Inactive Summary	External Tasks	
Split	Manual Task	External Milestone	
Milestone	Duration-only	Deadline	
Summary	Manual Summary Rollup	Progress	
Project Summary	Manual Summary	Manual Progress	
Inactive Task	Start-only		
Inactive Milestone	Finish-only		

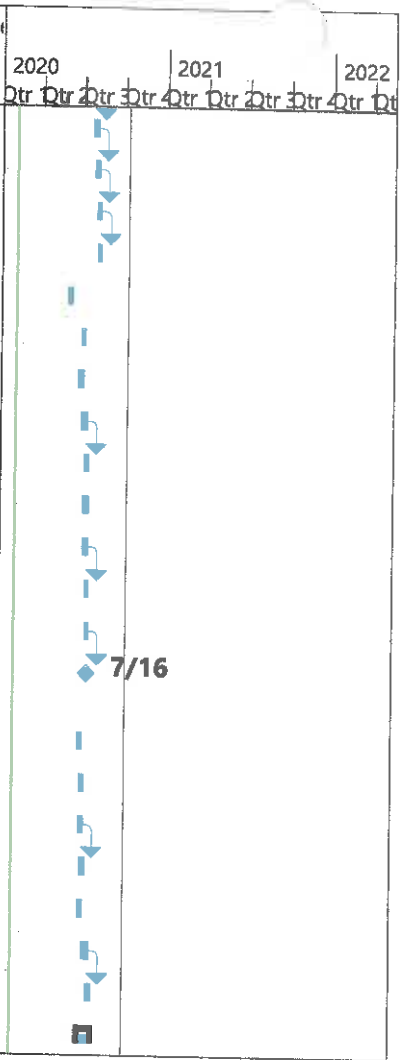
ID	Task N	Du	Start	Finish	Prede
207	Data Conversion Test Cases	10 days	Mon 5/11/20	Fri 5/22/20	184
208	Data Conversion Test Results	10 days	Tue 6/2/20	Mon 6/15/20	206
209	Identify Pilot Providers	6 days	Mon 6/8/20	Mon 6/15/20	
210	*Milestone 4 - Solution Design, Testing, and Operational Readiness 1 Complete*	*0 days*	*Tue 6/16/20*	*Tue 6/16/20*	*208*
211	Outreach and Communications	31 days	Wed 6/24/20	Wed 8/5/20	
212	**Email Blasts #1**	**16 days**	**Wed 6/24/20**	**Wed 7/15/20**	
213	Draft - Email Blast #1	6 days	Mon 4/27/20	Mon 5/4/20	
214	Deliver - Email Blast #1	1 day	Tue 5/5/20	Tue 5/5/20	213
215	Review - Email Blast #1	4 days	Wed 5/6/20	Mon 5/11/20	214
216	Revisions - Email Blast #1	2 days	Tue 5/12/20	Wed 5/13/20	215
217	Approval - Email Blast #1	3 days	Thu 5/14/20	Mon 5/18/20	216
218	Distribution - Email Blast #1	6 days	Tue 5/19/20	Tue 5/26/20	217
219	**Email Blasts #2**	**22 days**	**Mon 6/1/20**	**Tue 6/30/20**	
220	Draft - Email Blast #2	6 days	Mon 6/1/20	Mon 6/8/20	
221	Deliver - Email Blast #2	1 day	Tue 6/9/20	Tue 6/9/20	220
222	Review - Email Blast #2	4 days	Wed 6/10/20	Mon 6/15/20	221
223	Revisions - Email Blast #2	2 days	Tue 6/16/20	Wed 6/17/20	222
224	Approval - Email Blast #2	3 days	Thu 6/18/20	Mon 6/22/20	223
225	Distribution - Email Blast #2	6 days	Tue 6/23/20	Tue 6/30/20	224
226	**Email Blasts #3**	**15 days**	**Thu 7/16/20**	**Wed 8/5/20**	
227	Draft - Email Blast #3	5 days	Thu 7/16/20	Wed 7/22/20	
228	Deliver - Email Blast #3	1 day	Thu 7/23/20	Thu 7/23/20	227



Project: West Virginia Project
Plan Date: Wed 2/5/20

Task	Inactive Summary	External Tasks	
Split	Manual Task	External Milestone	
Milestone	Duration-only	Deadline	
Summary	Manual Summary Rollup	Progress	
Project Summary	Manual Summary	Manual Progress	
Inactive Task	Start-only		
Inactive Milestone	Finish-only		

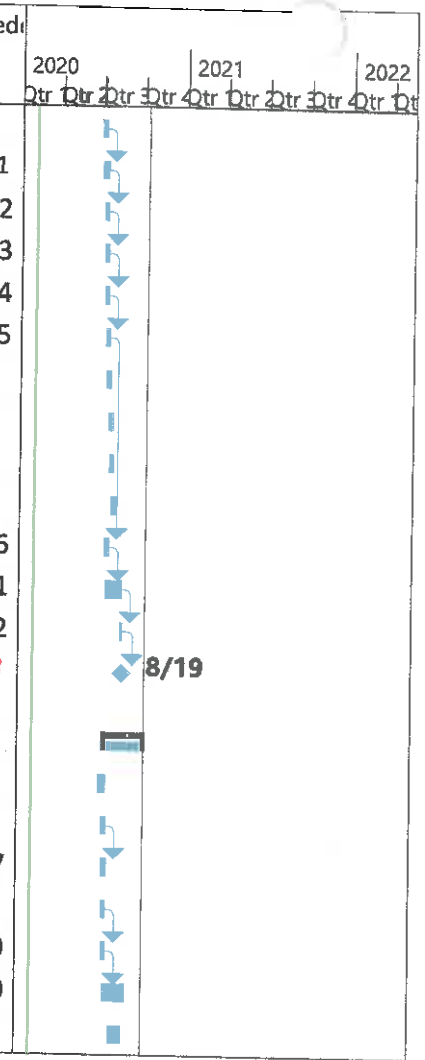
ID	Task N	Du	Start	Finish	Pred
229	Review - Email Blast #3	3 days	Fri 7/24/20	Tue 7/28/20	228
230	Revisions - Email Blast #3	3 days	Wed 7/29/20	Fri 7/31/20	229
231	Approval - Email Blast #3	2 days	Mon 8/3/20	Tue 8/4/20	230
232	Distribution - Email Blast #3	1 day	Wed 8/5/20	Wed 8/5/20	231
233	Federal Certification and Review Management Plan	3 days	*Mon 6/1/20*	*Wed 6/3/20*	
234	Interface Inventory	1 day	Fri 7/3/20	Fri 7/3/20	
235	Load and Stress Test Cases	4 days	Thu 6/25/20	Tue 6/30/20	
236	Load and Stress Testing	5 days	Fri 7/3/20	Thu 7/9/20	
237	Load and Stress Test Results	2 days	Fri 7/10/20	Mon 7/13/20	236
238	Operational Readiness Plan	4 days	Wed 7/8/20	Mon 7/13/20	
239	Operational Readiness Test Scripts	4 days	Wed 7/8/20	Mon 7/13/20	
240	Operational Readiness Test Results	1 day	Tue 7/14/20	Tue 7/14/20	239
241	System Demonstration	1 day	Wed 7/15/20	Wed 7/15/20	
242	*Milestone 5 - Solution Design, Testing, and Operational Readiness 2 Complete*	*0 days*	*Thu 7/16/20*	*Thu 7/16/20*	*241*
243	Reports and Forms Inventory	1 day	Thu 7/2/20	Thu 7/2/20	
244	System Integration Plan	3 days	Mon 7/6/20	Wed 7/8/20	
245	System Integration Test Cases	3 days	Mon 7/6/20	Wed 7/8/20	
246	System Integration Test Results	3 days	Thu 7/9/20	Mon 7/13/20	245
247	Regression Test Cases	3 days	Mon 7/6/20	Wed 7/8/20	
248	Regression Testing	7 days	Wed 7/15/20	Thu 7/23/20	
249	Regression Test Results	3 days	Fri 7/24/20	Tue 7/28/20	248
250	**Training Management Plan**	**22 days**	**Thu 7/2/20**	**Fri 7/31/20**	



Project: West Virginia Project
Plan Date: Wed 2/5/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

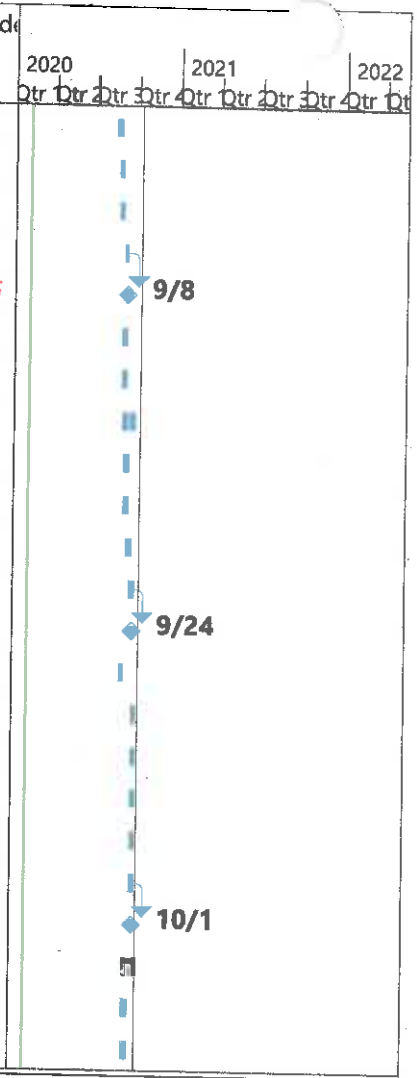
ID	Task N	Du	Start	Finish	Predi
251	Draft of Training Materials Delivered to DHHR	1 day	Thu 7/2/20	Thu 7/2/20	
252	Draft Training Materials Reviewed by DHHR	3 days	Fri 7/3/20	Tue 7/7/20	251
253	Marks/Comments Returned by DHHR	1 day	Wed 7/8/20	Wed 7/8/20	252
254	Training Materials Plan Revisions By Tellus	1 day	Thu 7/9/20	Thu 7/9/20	253
255	Revised Version of Training Materials Delivered to DHHR	1 day	Fri 7/10/20	Fri 7/10/20	254
256	DHHR Approval of Final Training Plan/Materials	1 day	Mon 7/13/20	Mon 7/13/20	255
257	On-site Training Module 1	2 days	Thu 7/16/20	Fri 7/17/20	
258	On-site Training Module 2	3 days	Mon 7/20/20	Wed 7/22/20	
259	On-site Training Module 3	2 days	Thu 7/23/20	Fri 7/24/20	
260	Webinar Training Modules 1, 2, 3 - July	5 days	Mon 7/27/20	Fri 7/31/20	
261	User Acceptance Test Cases	3 days	Tue 7/14/20	Thu 7/16/20	256
262	User Acceptance Testing	20 days	Fri 7/17/20	Thu 8/13/20	261
263	User Acceptance Test Results and Letter of Completion	3 days	Fri 8/14/20	Tue 8/18/20	262
264	*Milestone 6 - Solution Design, Testing, and Operational Readiness 3 Complete*	*0 days*	*Wed 8/19/20*	*Wed 8/19/20*	*263*
265	**Task Group 4 - Solution Deployment**	**62 days?**	**Tue 7/14/20**	**Wed 10/7/20**	
266	Implementation Plan (Rollout Plan)	6 days	Mon 7/6/20	Mon 7/13/20	
267	Production Environment Setup	1 day	Tue 7/14/20	Tue 7/14/20	
268	Data Load to Production	3 days	Wed 7/15/20	Fri 7/17/20	267
269	Production Environment Smoke Test	1 day	Thu 7/16/20	Thu 7/16/20	
270	System Go-Live	1 day?	Fri 7/17/20	Fri 7/17/20	269
271	Pilot Providers Begin Logging Visits and Submitting Claims	30 days	Mon 7/20/20	Fri 8/28/20	270
272	Webinar Training Modules 1, 2, 3 - August	15 days	Mon 8/3/20	Fri 8/21/20	



Project: West Virginia Project
Plan Date: Wed 2/5/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

ID	Task Name	Duration	Start	Finish	Predecessors
273	Cutover Play Book	3 days	Tue 8/18/20	Thu 8/20/20	
274	Implementation Certification Letter	1 day	Mon 8/24/20	Mon 8/24/20	
275	Federal Review Supporting Documentation	1 day	Mon 8/24/20	Mon 8/24/20	
276	Operations Change Management Plan	6 days	Mon 8/31/20	Mon 9/7/20	
277	*Milestone 7 - Deployment 1*	*0 days*	*Tue 9/8/20*	*Tue 9/8/20*	*276*
278	Operational Milestone Review	3 days	Mon 8/31/20	Wed 9/2/20	
279	Product Screenshots, Reports, and Data Certification	3 days	Mon 8/31/20	Wed 9/2/20	
280	Webinar Training Modules 1, 2, 3 - September	15 days	Wed 9/2/20	Tue 9/22/20	
281	Report Distribution Schedule	3 days	Mon 9/7/20	Wed 9/9/20	
282	Solution Health Monitoring Plan	3 days	Mon 9/7/20	Wed 9/9/20	
283	Report Distribution Schedule	3 days	Mon 9/14/20	Wed 9/16/20	
284	System Operations Plan	3 days	Mon 9/21/20	Wed 9/23/20	
285	*Milestone 8 - Deployment 2*	*0 days*	*Thu 9/24/20*	*Thu 9/24/20*	*284*
286	Mandatory Go-Live (eVV capture/claims submission)	1 day?	Tue 9/1/20	Tue 9/1/20	
287	System and User Documentation	3 days	Mon 9/28/20	Wed 9/30/20	
288	Training Materials	3 days	Mon 9/28/20	Wed 9/30/20	
289	Training Report	3 days	Mon 9/28/20	Wed 9/30/20	
290	Training Schedule	3 days	Mon 9/28/20	Wed 9/30/20	
291	Turnover and Closeout Management Plan	3 days	Mon 9/28/20	Wed 9/30/20	
292	*Milestone 9 - Deployment 3*	*0 days*	*Thu 10/1/20*	*Thu 10/1/20*	*291*
293	**Task Group 5 - Project Monitor and Control**	**18 days**	**Mon 9/14/20**	**Wed 10/7/20**	
294	Project Schedule	5 days	Mon 9/14/20	Fri 9/18/20	
295	Project Status Report (Weekly and Monthly)	5 days	Mon 9/14/20	Fri 9/18/20	

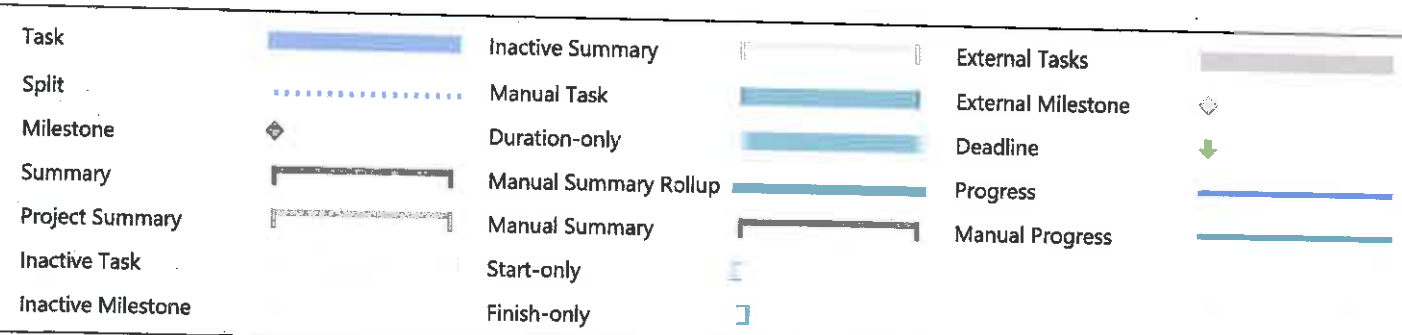


Project: West Virginia Project
Plan Date: Wed 2/5/20

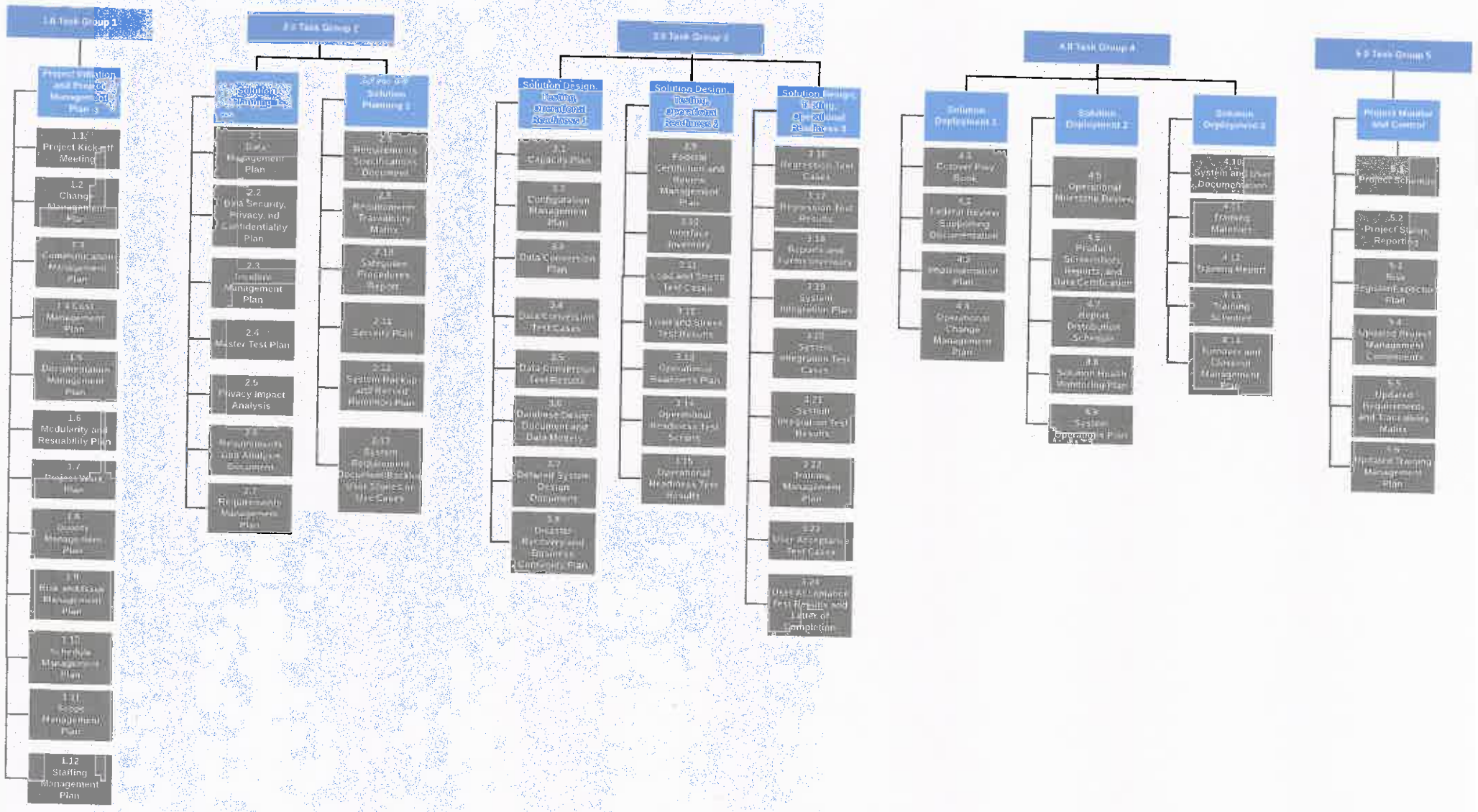
Task		Inactive Summary		External Tasks	
Split		Manual Task		External Milestone	
Milestone		Duration-only		Deadline	
Summary		Manual Summary Rollup		Progress	
Project Summary		Manual Summary		Manual Progress	
Inactive Task		Start-only			
Inactive Milestone		Finish-only			

ID	Task N	Du n	Start	Finish	Prede
296	Risk Register/Expection Plan	5 days	Mon 9/14/20	Fri 9/18/20	
297	Updated Project Management Components	5 days	Mon 9/14/20	Fri 9/18/20	
298	Updated Requirements Traceability Matrix	5 days	Thu 10/1/20	Wed 10/7/20	
299	Updated Training Management Plan	5 days	Thu 10/1/20	Wed 10/7/20	

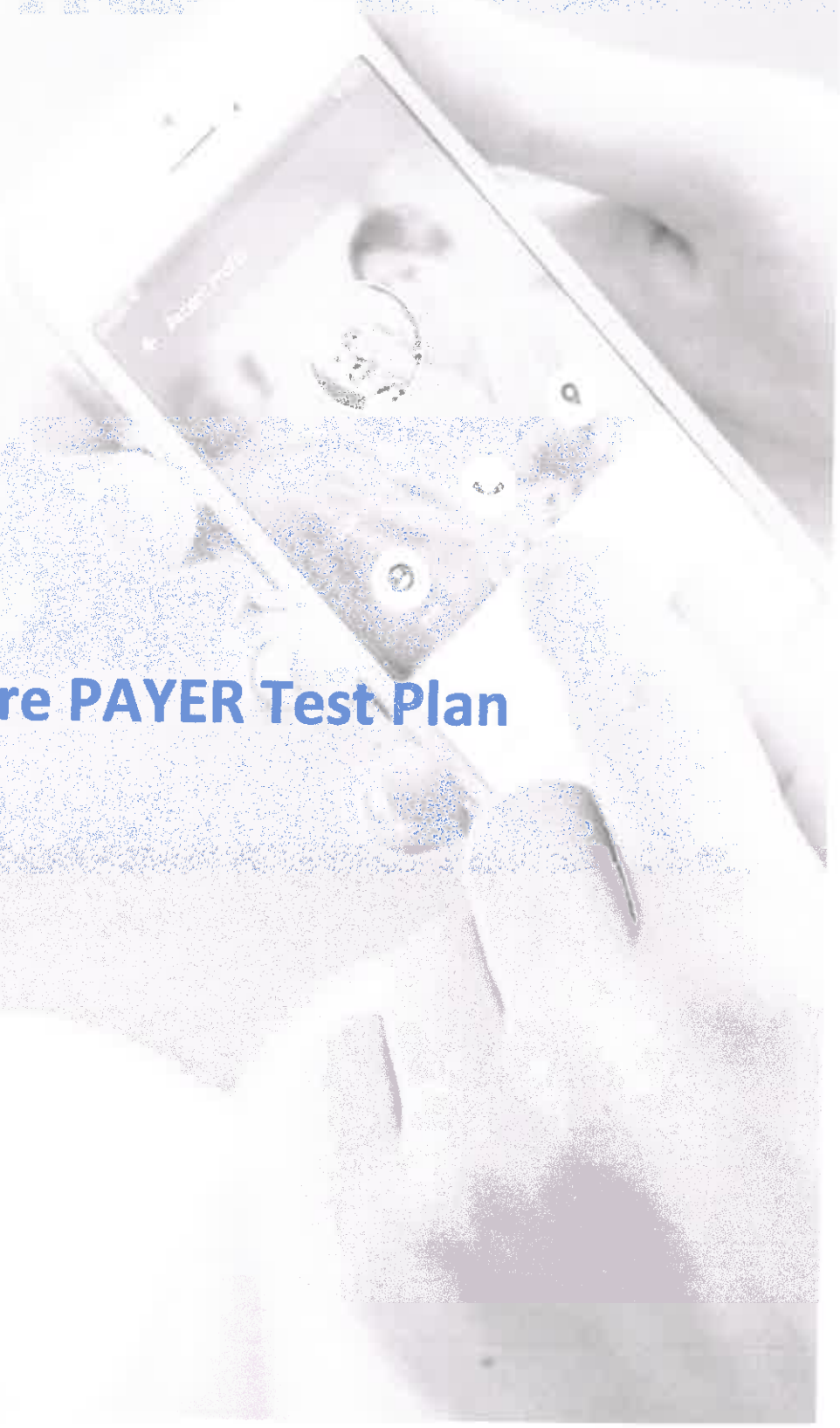
Project: West Virginia Project Plan Date: Wed 2/5/20



West Virginia Electronic Visit Verification Program



TELLUS



PayerNameHere PAYER Test Plan

Revision: 1.1
Date: March 10, 2020

TELLUS, LLC
800 Fairway Drive, #360
Deerfield Beach, FL 33441
(954) 719-0004
www.4tellus.com

STATEMENT OF CONFIDENTIALITY

This document contains confidential and proprietary information of Tellus, LLC ("Tellus") and is supplied to allow the recipient to make an evaluation of Tellus as a candidate for the delivery of software solutions and professional services. The recipient(s) of this document agree to inform present and future employees who receive or have access to this proposal of the confidential nature of this item and to instruct each employee not to disclose any information concerning this document to others without prior written consent from a duly authorized Tellus representative. The recipient further agrees to protect said confidential information as internal confidential information would be protected and not to disclose any information concerning this document to others without prior written consent from a duly authorized Tellus representative. The recipient of this document agrees not to duplicate or permit others to duplicate any material contained hereunder except for internal use.

REVISION HISTORY

NAME	REVISION DATE	VERSION	DESCRIPTION OF CHANGES
			Initial Draft

Table of Contents

1. INTRODUCTION 4
   1.1. REFERENCES & RELATED DOCUMENTS 5
2. PROJECT MANAGEMENT OVERVIEW 5
   2.1. ACTIVITIES BY PHASE 5
   2.2. KEY DELIVERABLES BY PHASE 6
   2.3. ENVIRONMENTS 7
   2.4. PROJECT STAFFING 10
3. TEST SCHEDULE AND GOVERNANCE 10
   3.1. TEST PLANNING 10
   3.2. TEST SCHEDULE 11
   3.3. REQUIRED TESTING RESOURCES 11
   3.4. UAT ENTRANCE CRITERIA 12
   3.5. UAT TEST RELEASE CRITERIA 12
   3.6. REQUIREMENTS TRACEABILITY CONFORMANCE 13
4. TEST STRATEGY 13
   4.1. FUNCTIONAL TEST OBJECTIVES & SCOPE 13
      4.1.1. Prior Authorization (PA) Objectives 13
      4.1.2. Provider Messaging Text Objectives 17
      4.1.3. Recipient Objectives 19
      4.1.4. Claims Messaging Test Objectives 20
      4.1.5. Visit Management Test Objectives 24
5. DEFECT MANAGEMENT 25
6. APPROVALS 26
7. APPENDIX A - ACRONYMS & DEFINITION OF TERMS 27
   7.1. ACRONYMS 27
   7.2. DEFINITION OF TERMS 27

1. INTRODUCTION

This document is the Test Plan for the Payer MCO Integration to the Electronic Visit Verification (eVV) platform. It identifies the project objectives, deliverables, resource requirements and risks associated with managing the testing of this project. Progress will be tracked with the Jira and test coverage metric reports.

The testing program for this integrated solution will address the following functional areas:

1. Prior Authorization (PA) Messaging Test Objectives:
   1.1. Inbound Process New PA.
   1.2. Inbound Additional PA for Recipient - Same PA #.
   1.3. Inbound Additional PA for Recipient - Different PA #.
   1.4. Adjust Existing PA.
   1.5. Error PA - Overlapping Dates.
   1.6. Rejected PA – Missing Required Fields.
2. Provider Messaging Test Objectives:
   2.1. Create New Provider.
   2.2. Update Existing Provider.
   2.3. Make Existing Provider Ineligible.
3. Recipient Messaging Test Objectives:
   3.1. Create New Recipient.
   3.2. Update Existing Recipient.
   3.3. Make Existing Recipient Ineligible.
4. Claims Messaging Test Objectives:
   4.1. Claims Submission via 837P (New Claim) Completed by Tellus.
   4.2. Claims Submission via 837P (New Claim) processed by Payer.
   4.3. Claims Submission via 837P (Void Claim) Completed by Tellus.
   4.4. Claims Submission via 837P (Void Claim) processed by Payer.
   4.5. Claims Submission via 837P (Adjusted Claim) Completed by Tellus.
   4.6. Claims Submission via 837P (Adjusted Claim) processed by Payer.
   4.7. Claims Submission via 837P (Denied Claim Resubmitted) Completed by Tellus.
   4.8. Claims Submission via 837P (Denied Claim Resubmitted) processed by Payer.
   4.9. 999 generated by Payer
   4.10. 277 generated by Payer
   4.11. 835 (or 835 equivalent) generated by Payer
   4.12. 999 Processed by Tellus.
   4.13. 835 Processed by Tellus (Full Payment).
   4.14. 835 Processed by Tellus (Partial Payment).

4.15. 835 Processed by Tellus (Denial).

4.16. Overnight Claim Spanning Midnight.

5. Visit Management Test Objectives

5.1. Overnight Visit

5.2. Multiple Recipients on a Single Visit - No TT Modifier

5.3. Multiple Recipients on a Single Visit - With TT Modifier

5.4. Multiple Service Code on a Single Visit

5.5. GPS Maximum Range between Scheduled and Actual Start

5.6. Completed Late Visit

1.1. REFERENCES & RELATED DOCUMENTS

Table 1: Related Documents

DOCUMENT TITLE	DOCUMENT NO.	REVISION
Tellus eVV Payer Implementation Guide		
Payer Integration Specification		
Payer UAT - Inbound Provider File Validation		
Payer UAT - Inbound Prior Authorization File Validation		
Payer UAT - Inbound Recipient File Validation		

2. PROJECT MANAGEMENT OVERVIEW

2.1. ACTIVITIES BY PHASE

The following activities will be carried out by phase of the project. See highlighted for items specific to testing:

Table 2: Activities by Project Phase

Phase	Activities
Prior to Start	• Contracts Signed. • Teams introduced, and roles assigned. • Project management approach agreed. • Standard documentation review.
Requirements Gathering	• Kick off meeting, typically onsite at Tellus or client site. • Requirements completed for any product enhancement requests or non-standard integration. • Any product enhancement change orders presented and executed.

Design	• Tellus and Client BA's coordinate with their respective architects and technology teams to design solution per the given requirements.
Construction	• Tellus and Client technology teams write the software. • User outreach and training typically starts during development but may begin earlier or later depending up scheduling details. • Test plan written jointly by Tellus and Payer.
QA	• Tellus and Client quality teams each QA- and regression- test their respective software deliveries. Note: Tellus uses continuous integration (CI) build-deploy so that all software checked in is automatically deployed to QA. • Full Tellus-Client integration testing begins with QA. • The goal of QA is to deliver a production-ready software solution into the UAT environment.
UAT	• Client acceptance tests the complete integrated solution. • Client sign-off on production acceptance.
Production	• Release of the production solution into a production environment.

2.2. KEY DELIVERABLES BY PHASE

The following are key deliverables that Tellus will delivery by sprint/phase.

Table 3: Key Deliverables by Project Phase

Phase	Deliverables

Prior to Start	• Product Implementation Guide (This Document).
	• Standard Integration Specifications (online):
	  ○ Data Dictionary.
	  ○ Sample Messages (Flat File and XML).
	  ○ XML Schema.
	• Product Technical Specifications.
	• Product User Guide.
	• Draft schedule.

Throughout the Project	• Updated task list that includes:
	  ○ Task.
	  ○ Reporter.
	  ○ Assignee.
	  ○ Due Date.
	  ○ Next steps.
	• Updated listing of open issues/defects.
	• Updated delivery schedule/sprint schedule.

End of Requirements Gathering	• Change Orders for any billable work:
	  ○ Recital of requirements.
	  ○ Proposed solution.
	  ○ Costs.
	  ○ Timeline impacts.
	• Client Implementation Document (DRAFT):
	  ○ Integration Specifications for any non-standard integration.
	  ○ Listing of client-requested product enhancements (change orders).

End of Design	• Any design updates to change orders or the Client Implementation Document.
End of Construction	• Unit- and Integration-tested software deployment into quality assurance (QA) environment. • Any updates to change orders or the Client Implementation Document. • Test plan written jointly by Tellus and Payer.
End of QA	• QA and regression-tested solution deployed into UAT environment, ready for user acceptance testing (UAT). • Any updates to change orders or the Client Implementation Document.
End of UAT	• UAT-tested and accepted software solution ready for deployment into a production environment. • Any as-built updates to change orders or the Client Implementation Document (Final).
In Production	• Production software solution deployed into a production environment. • Ongoing training and outreach per Master Software and Services agreement. • Ongoing Tier-1 and/or Tier-2 user support per Master Software and Services agreement. • Ongoing B-2-B Operations Support per Master Software and Services agreement. • Ongoing hosting per Master Software and Services agreement.

2.3. ENVIRONMENTS

Tellus operates the following environments for our software development lifecycle (SDLC):

Development (DEV)

- Environment used by developers to write source code, configure databases, etc.
- Developers use NetBeans Integrated Development Environment (IDE)
- Source code managed using BitBucket Distributed version control system.
- DEV deployments are made back into the dev environment for unit and integration testing.

Quality Assurance (QA)

- Environment used by Tellus QA testers for quality assurance and regression testing.
- Take continuous integration builds as developers check software into Git.
- QA Mobile devices with iOS operating system take releases from TestFlight, an Apple App Store analogue used for testing purposes.
- QA Mobile devices with Android operating system receive Android application package (APK) releases buy internal email from Tellus Build-Deploy manager.
- Tellus and client begin full integration testing in QA, so client should be ready to integrate QA environments.
- The goal is to address all issues in QA, deploying only production-ready software to UAT.

User Acceptance Testing (UAT)

- Environment used by Tellus UAT testers for quality assurance, regression, and smoke testing at times.
- Environment used by client UAT testers for integration and acceptance testing.
- QA Mobile devices with iOS operating system take releases from TestFlight.
- QA Mobile devices with Android operating system receive APK releases buy internal email from Tellus Build-Deploy manager.
- Tellus and client continue full integration testing in UAT.
- All production-blocker defects must be addressed in QA before a production deployment.

Production (PROD)

- Reserved for only fully-tested production releases.

Demo (DEMO)

- Used for demonstration and training purposes only.
- Typically takes production releases only.
- Has a preconfigured suite of demo data that is automatically restored each night to allow for a "clean" demo/test environment each day.

The following diagram illustrates the Tellus infrastructural organization.

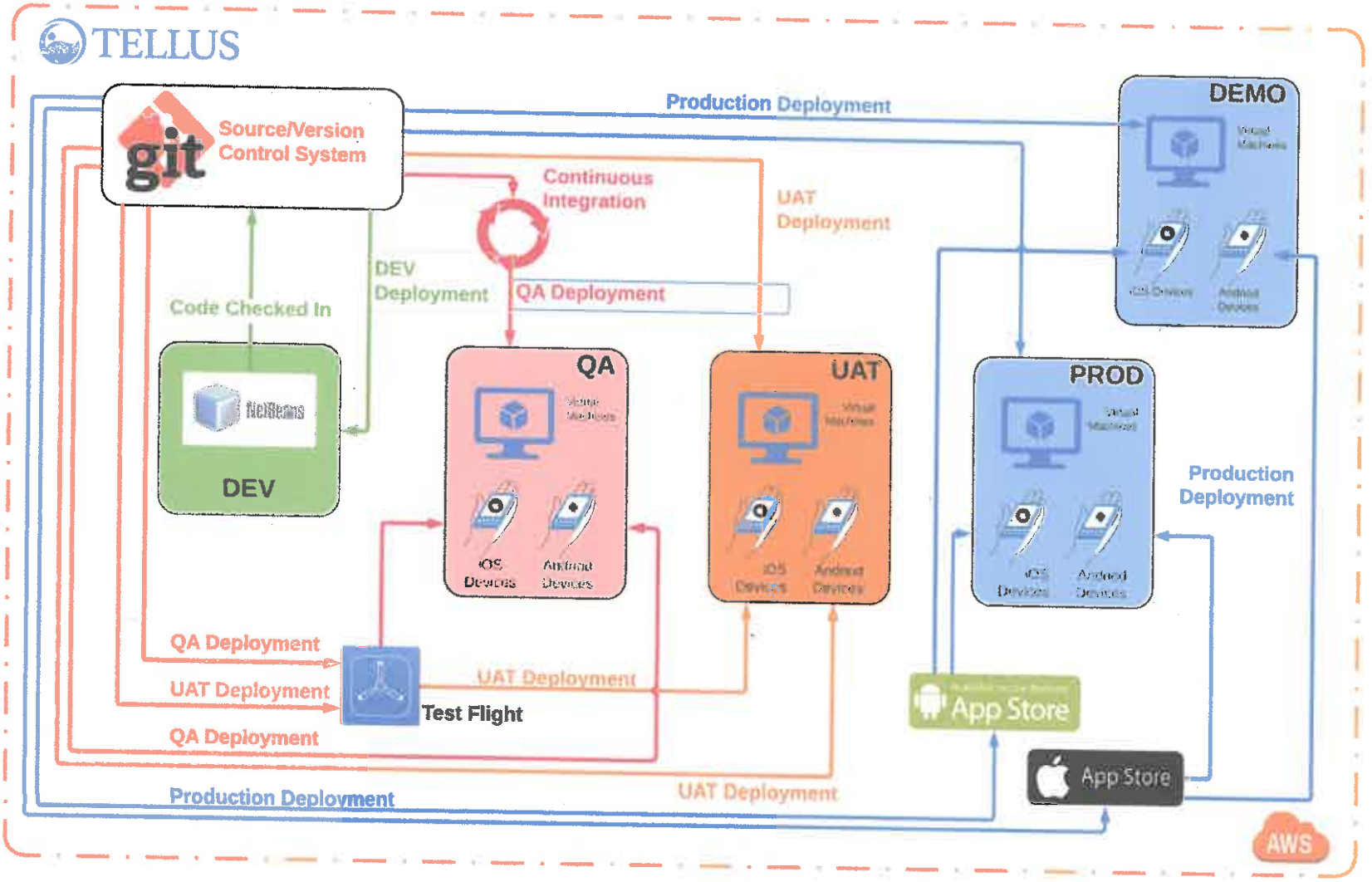


Figure 1: Tellus SDLC Infrastructure Diagram

2.4. PROJECT STAFFING

Tellus will staff each project according to requirements, but the general "package" is as follows:

Position	Description	Staffing
Senior Business Stakeholder	Senior manager who monitors the project, coordinates with client senior managers, and acts as an escalation point for any issues that may arise.	.1 Full Time Employee (FTE)
Solution Architect	Provides technical leadership with a focus on the vetting and design of any enhancement requests and any non-standard integration.	.1 FTE
Project Manager (PM)/Scrum Master (SM)	Provides project leadership, including: Single point of contact for the client, the management of task lists, the management of project schedule, management of project risks, the first line of resolution in any project issues, liaison between all other project participants.	.25 FTE
Business Analyst (BA)	The liaison between the business and technical teams. Focused on technical documentation including business requirements, use cases, functional specifications, data maps, etc.	1 FTE
Developers	A team of software developers of varying specialties.	1-2 FTE
Test Engineers	Tellus manages an ongoing quality assurance/quality control program that includes a full suite of new feature testing and regression testing on each release.	1-2 FTE

Payer staffing will depend on the details of the project, but if client-side software development is necessary, then the client team should roughly mirror the Tellus team. At minimum the client team will require a project manager to act as the single point of contact for Tellus, and to act as the coordinator of client-side staff.

3. TEST SCHEDULE AND GOVERNANCE

3.1. TEST PLANNING

Integrated testing will begin during the QA cycle, so planning for integration (FTP servers, test harnesses if necessary, etc.) must be completed during the development phase.

Notes on Preparation for Testing:

1. Please review the **Activities by Phase** and **Deliverables by Phase** sections above to understand the activities for QA vs. UAT testing.
2. Tellus will coordinate with you on test planning during the Development Phase.
3. See the **Environments** section above. Tellus will coordinate with you during the requirements phase to align Tellus-Payer environments.

Test Data Requirements:

1. Tellus does not allow for production data that contains PHI (Private Health Information), also known as personally identifiable information (PII) or non-public information (NPI) in any test environment. This means that you must be prepared to begin integration testing with scrubbed test data.
2. Plan to be ready to transmit test data via integrated channel (web services, FTP, etc.) by the beginning of the QA cycle.
3. Please plan for a daily test runs, or per the schedule that you agree with Tellus.
4. Data transmitted from Payer to Tellus is typically focused around recipient, prior authorization, and provider data sets. It is important that you create coordinated test data, so that the PA data aligns with the recipient and provider test data.
5. After Tellus receives the Payer test data, we will run test eVV visits and begin to generate claims data to return to your test systems. Please ensure that your recipient, prior authorization, and provider data sets contain sufficient variation to cover your test cases.

3.2. TEST SCHEDULE

Please refer to the project Gantt chart for QA and UAT test cycle dates.

3.3. REQUIRED TESTING RESOURCES

Testing will be performed by the Tellus and Payer Quality Assurance Test Teams. Test Engineers will be responsible for test case development, execution of tests, opening defect reports upon observance of nonconformance to documented requirements.

1. **Payer will be responsible for:**
   - 1.1. Generating test data for the recipient, provider, and PA feeds per this test plan and transmitting this data to Tellus.
   - 1.2. Receiving and processing 837P claims submission files from Tellus, including claims adjudication.
   - 1.3. Returning 999 and 835 (or agreed upon surrogate) files to Tellus for each 837P file transmitted by Tellus.
   - 1.4. Reporting any issues that may pertain to Tellus systems in a mutually agreed written softcopy format (typically a spreadsheet).
   - 1.5. Tracking and addressing any issues reported as pertaining to Payer systems using a mutually-agreed format (typically a spreadsheet).

2. **Tellus will be responsible for:**

2.1. Receiving and processing the recipient, provider, and PA feeds transmitted by Payer.

2.2. Generating and transmitting 837P claims submission files to Payer. This includes the scheduling, completion, and pre-adjudication of all test visits using the Tellus eVV platform.

2.3. Receiving and processing 999 and 835 (or agreed upon surrogate) files from Payer for each 837P file transmitted by Tellus.

2.4. Reporting any issues that may pertain to Payer systems in a mutually agreed written softcopy format (typically a spreadsheet).

2.5. Tracking and addressing any issues reported as pertaining to Tellus systems using a mutually-agreed format (typically a spreadsheet).

3.4. UAT ENTRANCE CRITERIA

Testing will begin at the direction of test management. The following criteria must be achieved prior to starting the UAT Testing Cycle.

- Requirements are defined and approved
- Completed testable code is available
- Test cases are developed and ready
- UAT test environment has been set-up and all other necessary resources are available
- Sufficient test data has been loaded into the test environment
- All known existing Top Priority defects have been resolved
- Smoke Testing has been executed and passed 100%

3.5. UAT TEST RELEASE CRITERIA

This section defines the targeted goals and conformance to exit UAT. Below are the UAT Exit Criteria:

Table 4: UAT Exit Criteria

REQUIREMENTS TRACEABILITY
All Planned Requirements have been Implemented & Delivered
All Requirements have been Tested
ACCEPTANCE TESTING

100% Test Case execution of all Acceptance Test Cases
100% Pass Rate of all Acceptance Test Cases

3.6. REQUIREMENTS TRACEABILITY CONFORMANCE

All Test Case to requirements traceability will be managed in Jira. Jira is an agile project management tool for creating and managing user stories, tasks, test cases, and defects.

4. TEST STRATEGY

4.1. FUNCTIONAL TEST OBJECTIVES & SCOPE

The purpose of this Test Plan is to define the testing objectives and overall testing approach for the Payer MCO v2.0 Integration with the Tellus Electronic Visit Verification (eVV) platform.

The approach of this testing effort is from an interface perspective, which is the operation of features and functions from external interfaces, which include the user interface and API interface. The primary focus will be black-box oriented; however, structural-testing techniques may be used to simulate environmental conditions and verify 'hidden' functions. Test types will include positive, negative, and error recovery.

The objectives for this testing effort are outlined below:

4.1.1. PRIOR AUTHORIZATION (PA) OBJECTIVES

4.1.1.1. Inbound Process New PA

Prerequisite: Provider and Recipient data used in test PA records already processed by Mirth and in the Payer database schema.

Objective: Validate Mirth "AAAA Processor Prior Authorization" channel processes the prior authorization file as a new prior authorization in the database.

Test Scope: The following scenarios are created from our Inbound Data Matching requirements for PA records. Scenarios are based on the logic for the following key data points in the PA record: PayerProviderId, RecipientMedicaidId, ServiceCode (including ServiceCodeMod1 and ServiceCodeMod2). If any of the key data points are not found in an existing database PA record, then a new PA record is created in the database. If all of the key data points match an existing database PA record, then the PayerAuthId and the AuthEffDate and AuthExpDate data range are evaluated. If the PayerAuthId does not match the existing PA record and AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. If the PayerAuthId does match the existing PA record and the AuthEffDate and AuthExpDate

date range does not overlap, then a new PA record is created in the database. After a PA batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the PA batch file, the number of PA records accepted, and the number of PA records rejected. Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the PA batch file with error codes and error descriptions for reconciliation by the client.

Notes: Tellus staff see the following link for inbound PA matching logic scenarios:

https://tellusolutions.atlassian.net/wiki/spaces/EVV/pages/488013832/Inbound+Data+Matching

4.1.1.2. Inbound Process Additional PA for Recipient - Same PA Number

Prerequisite: Provider and Recipient data used in test PA records already processed by Mirth and in the Payer database schema.

Objective: Validate Mirth "AAAA Processor Prior Authorization" channel processes the prior authorization file as an additional PA for same provider, recipient, service code, & PA number, but with a different non-overlapping date range.

Test Scope: The following scenarios are created from our Inbound Data Matching requirements for PA records. Scenarios are based on the logic for the following key data points in the PA record: PayerProviderId, RecipientMedicaidId, ServiceCode (including ServiceCodeMod1 and ServiceCodeMod2). If any of the key data points are not found in an existing database PA record, then a new PA record is created in the database. If all of the key data points match an existing database PA record, then the PayerAuthId and the AuthEffDate and AuthExpDate data range are evaluated. If the PayerAuthId does not match the existing PA record and AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. If the PayerAuthId does match the existing PA record and the AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. After a PA batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the PA batch file, the number of PA records accepted, and the number of PA records rejected. Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the PA batch file with error codes and error descriptions for reconciliation by the client.

Notes: Tellus staff see the following link for inbound PA matching logic scenarios:

https://tellusolutions.atlassian.net/wiki/spaces/EVV/pages/488013832/Inbound+Data+Matching

4.1.1.3. Inbound Process Additional PA for Recipient - Different PA Number

Prerequisite: Provider and Recipient data used in test PA records already processed by Mirth and in the Payer database schema.

Objective: Validate Mirth "AAAA Processor Prior Authorization" channel processes the prior authorization file as an additional PA for same provider, recipient, service code, with different PA number and a different non-overlapping date range.

Test Scope: The following scenarios are created from our Inbound Data Matching requirements for PA records. Scenarios are based on the logic for the following key data points in the PA record: PayerProviderId, RecipientMedicaidId, ServiceCode (including ServiceCodeMod1 and ServiceCodeMod2). If any of the key data points are not found in an existing database PA record, then a new PA record is created in the database. If all of the key data points match an existing database PA record, then the PayerAuthId and the AuthEffDate and AuthExpDate data range are evaluated. If the PayerAuthId does not match the existing PA record and AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. If the PayerAuthId does match the existing PA record and the AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. After a PA batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the PA batch file, the number of PA records accepted, and the number of PA records rejected. Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the PA batch file with error codes and error descriptions for reconciliation by the client.

Notes: Tellus staff see the following link for inbound PA matching logic scenarios:

https://tellusolutions.atlassian.net/wiki/spaces/EVV/pages/488013832/Inbound+Data+Matching

4.1.1.4. Adjust Existing PA

Prerequisite: Provider and Recipient data used in test PA records already processed by Mirth and in the Payer database schema.

Objective: Validate Mirth "AAAA Processor Prior Authorization" channel processes the prior authorization file as an additional PA for same provider, recipient, service code, & PA number the same or a different overlapping date range.

Test Scope: The following scenarios are created from our Inbound Data Matching requirements for PA records. Scenarios are based on the logic for the following key data points in the PA record: PayerProviderId, RecipientMedicaidId, ServiceCode (including ServiceCodeMod1 and ServiceCodeMod2). If any of the key data points are not found in an existing database PA record, then a new PA record is created in the database. If all of the key data points match an existing database PA record, then the PayerAuthId and the AuthEffDate and AuthExpDate data range are evaluated. If the PayerAuthId does not match the existing PA record and AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. If the PayerAuthId does match the existing PA record and the AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. After a PA batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the PA batch file, the number of PA records accepted,

and the number of PA records rejected. Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the PA batch file with error codes and error descriptions for reconciliation by the client.

Notes: Tellus staff see the following link for inbound PA matching logic scenarios:

https://tellusolutions.atlassian.net/wiki/spaces/EVV/pages/488013832/Inbound+Data+Matching

4.1.1.5. Error PA – Overlapping Dates

Prerequisite: Provider and Recipient data used in test PA records already processed by Mirth and in the Payer database schema.

Objective: Validate Mirth "AAAA Processor Prior Authorization" channel processes the prior authorization file as an additional PA for same provider, recipient, service code, but different PA number the same or a different overlapping date range. This is an error condition, PA's that meet these conditions are treated as duplicates.

Test Scope: The following scenarios are created from our Inbound Data Matching requirements for PA records. Scenarios are based on the logic for the following key data points in the PA record: PayerProviderId, RecipientMedicaidId, ServiceCode (including ServiceCodeMod1 and ServiceCodeMod2). If any of the key data points are not found in an existing database PA record, then a new PA record is created in the database. If all of the key data points match an existing database PA record, then the PayerAuthId and the AuthEffDate and AuthExpDate data range are evaluated. If the PayerAuthId does not match the existing PA record and AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. If the PayerAuthId does match the existing PA record and the AuthEffDate and AuthExpDate date range does not overlap, then a new PA record is created in the database. After a PA batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the PA batch file, the number of PA records accepted, and the number of PA records rejected. Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the PA batch file with error codes and error descriptions for reconciliation by the client.

Notes: Tellus staff see the following link for inbound PA matching logic scenarios:
https://tellusolutions.atlassian.net/wiki/spaces/EVV/pages/488013832/Inbound+Data+Matching

4.1.1.6. Rejected PA – Missing Required Fields

Prerequisite: Existing and non-existing provider and recipient records in the Tellus payer, provider, and recipient, database tables depending on the test case scenarios.

Objective: Validate Mirth "AAAA Processor Prior Authorization" channel processes the prior authorization file and rejects the record if the provider or recipient does not already exist in the payer, provider, or recipient database tables.

Test Scope: PA records are rejected in the following scenarios (non-existing means not in the Tellus payer database table and existing means is in the Tellus payer database table):

1. The PA record has a non-existing PayerProviderId and an existing RecipientMedicaidId
2. The PA record has an existing PayerProviderId and a non-existing RecipientMedicaidId
3. The PA record has a non-existing PayerProviderId and a non-existing RecipientMedicaidId

After a PA batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the PA batch file, the number of PA records accepted, and the number of PA records rejected. Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the PA batch file with error codes and error descriptions for reconciliation by the client.

4.1.2. PROVIDER MESSAGING TEXT OBJECTIVES

4.1.2.1. Create New Provider

Prerequisite: Provider does not already exist in Tellus payer database schema.

Objective: Validate Mirth "AAAA Processor Provider" channel processes the provider file as a new provider in the Tellus payer specific database schema.

Test Scope: A new provider record is created with data in the provider file if the provider does not already exist in Tellus payer database schema. Provider already existing or not existing is determined based on whether the PayerProviderId field value in the file is found or not found in the Tellus payer specific database schema. After a Provider batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the Provider batch file, the number of provider records accepted, the number of provider records accepted that were new records, the total number of provider records accepted that were updated records, the number of provider records rejected, and the current total of provider records in the payer specific provider database (including the records from the batch that generated the provider results email). Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the Provider batch file with error codes and error descriptions for reconciliation by the client.

4.1.2.2. Update Existing Provider

Prerequisite: Provider already exists in Tellus payer database schema.

Objective: Validate Mirth "AAAA Processor Provider" channel processes the provider file with an update to an existing provider record in the Tellus payer specific database schema.

Test Scope: A provider record is updated with the data in the provider file if the provider already exists in the Tellus payer database schema. Provider already existing or not existing is determined based on whether the PayerProviderId field value in the file is found or not found in the Tellus payer specific database schema. After a Provider batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the Provider batch file, the number of provider records accepted, the number of provider records accepted that were new records, the total number of provider records accepted that were updated records, the number of provider records rejected, and the current total of provider records in the payer specific provider database (including the records from the batch that generated the provider results email). Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the Provider batch file with error codes and error descriptions for reconciliation by the client.

4.1.2.3. Make Existing Provider Ineligible

Prerequisite: Provider already exists in Tellus payer database schema.

Objective: Validate Mirth "AAAA Processor Provider" channel processes the provider file with an update to an existing provider record in the Tellus payer specific database schema to make the provider ineligible (disabled, no logins allowed) on Tellus eVV system.

Test Scope: A provider record that contains a populated ProviderExpDate that is <= current date, then the provider and the provider's caregivers should be disabled from accessing the Tellus eVV platform. After a Provider batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the Provider batch file, the number of provider records accepted, the number of provider records accepted that were new records, the total number of provider records accepted that were updated records, the number of provider records rejected, and the current total of provider records in the payer specific provider database (including the records from the batch that generated the provider results email). Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the Provider batch file with error codes and error descriptions for reconciliation by the client.

4.1.3. RECIPIENT OBJECTIVES

4.1.3.1. Create New Recipient

Prerequisite: Recipient does not already exist in Tellus payer database schema.

Objective: Validate Mirth "AAAA Processor Recipient" channel processes the recipient file as a new recipient in the Tellus payer specific database schema.

Test Scope: A new recipient record is created with data in the recipient file if the recipient does not already exist in the Tellus payer database schema. Recipient already existing or not existing is determined based on whether the RecipientMedicaidId field value in the file is found or not found in the Tellus payer specific schema. After a Recipient batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the Recipient batch file, the number of recipient records accepted, the number of recipient records accepted that were new records, the total number of recipient records accepted that were updated records, the number of recipient records rejected, and the current total of recipient records in the payer specific recipient database (including the records from the batch that generated the recipient results email). Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the Recipient batch file with error codes and error descriptions for reconciliation by the client.

4.1.3.2. Update Existing Recipient

Prerequisite: Recipient does not already exist in Tellus payer database schema.

Objective: Validate Mirth "AAAA Processor Recipient" channel processes the recipient file with an update to an existing recipient record in the Tellus payer specific database schema.

Test Scope: A recipient record is updated with the data in the recipient file if the recipient already exists in the Tellus payer database schema. Recipient already existing or not existing is determined based on whether the RecipientMedicaidId field value in the file is found or not found in the Tellus payer specific schema. After a Recipient batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the Recipient batch file, the number of recipient records accepted, the number of recipient records accepted that were new records, the total number of recipient records accepted that were updated records, the number of recipient records rejected, and the current total of recipient records in the payer specific recipient database (including the records from the batch that generated the recipient results email). Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the Recipient batch file with error codes and error descriptions for reconciliation by the client.

4.1.3.3. Make Existing Recipient Ineligible

Prerequisite: Recipient already exists in Tellus payer database schema.

Objective: Validate Mirth "AAAA Processor Provider" channel processes the provider file with an update to an existing provider record in the Tellus payer specific database schema to make the recipient ineligible (scheduling disallowed, start visit disallowed) on Tellus eVV system.

Test Scope: A recipient record that contains a populated EligibilityEndDate that is <= current date, then the recipient should be disabled (scheduling disallowed, start visit disallowed) on the Tellus eVV platform. After a Recipient batch file is processed by Mirth a results email is sent to the subscriber(s). The results email will have the total number of records processed in the Recipient batch file, the number of recipient records accepted, the number of recipient records accepted that were new records, the total number of recipient records accepted that were updated records, the number of recipient records rejected, and the current total of recipient records in the payer specific recipient database (including the records from the batch that generated the recipient results email). Mirth also creates an accepted and rejected file in the client sftp outbound folder with detailed results. The rejected file will have each rejected record from the Recipient batch file with error codes and error descriptions for reconciliation by the client.

4.1.4. CLAIMS MESSAGING TEST OBJECTIVES

4.1.4.1. Claims Submission via 837P (New Claim) Completed by Tellus

Prerequisite: Claim is in "Matched" status on the eVV Work List screen.

Objective: Validate that a Matched Claim can be submitted and generate an 837P Claims File.

Test Scope: A Provider Administrator can "release" a matched claim. Status is displayed as RELEASED. The "Released" claim is processed and an 837P Claims file is generated and sent to Payer. Once the claim is processed, the claim status will display as SUBMITTED.

4.1.4.2. Claims Submission via 837P (New Claim) processed by Payer

Prerequisite: Payer receives an 837P Claims File (New Claim).

Objective: Validate that an 837P Claims File (New Claim) is received, processed, accepted and an EDI 999 File (Implementation Acknowledgement) is generated and sent to Tellus eVV.

Test Scope: An 837P Claim File (New Claim) is received, processed, accepted and an EDI 999 File (Implementation Acknowledgement) responds with one of the following scenarios, 1) Accepted (no errors), 2) Accepted (with errors), or Rejected. If the 999 is Accepted with errors or Rejected, Payer's claims processing system responds with an EDI 835 (Health Care Claim Payment/Advice).

4.1.4.3. Claims Submission via 837P (Void Claim) Completed by Tellus.

Prerequisite: Claim is in "Paid" or "Denied" status on the eVV Work List screen.

Objective: Validate that a void claim transaction can be submitted and generate an 837P Claims File.

Test Scope: A Provider Administrator can "release" a void claim. Status is displayed as RELEASED. The "Released" claim is processed and an 837P Claims file is generated and sent to Payer. Once the claim is processed, the claim status will display as SUBMITTED.

4.1.4.4. Claims Submission via 837P (Void Claim) processed by Payer.

Prerequisite: Payer receives an 837P Claims File (Void Claim).

Objective: Validate that an 837P Claims File (Void Claim) is received, processed, accepted and an EDI 999 File (Implementation Acknowledgement) is generated and sent to Tellus eVV.

Test Scope: An 837P Claim File (Void Claim) is received, processed, accepted and an EDI 999 File (Implementation Acknowledgement) responds with one of the following scenarios, 1) Accepted (no errors), 2) Accepted (with errors), or Rejected. If the 999 is Accepted with errors or Rejected, Payer's claims processing system responds with an EDI 835 (Health Care Claim Payment/Advice).

4.1.4.5. Claims Submission via 837P (Adjusted Claim) Completed by Tellus.

Prerequisite: Claim is in "Paid" or "Denied" status on the eVV Work List screen.

Objective: Validate that an adjusted claim transaction can be submitted and generate an 837P Claims File.

Test Scope: A Provider Administrator can "release" an adjusted claim. Status is displayed as RELEASED. The "Released" claim is processed and an 837P Claims file is generated and sent to Payer. Once the claim is processed, the claim status will display as SUBMITTED.

4.1.4.6. Claims Submission via 837P (Adjusted Claim) processed by Payer.

Prerequisite: Payer receives an 837P Claims File (Adjusted Claim).

Objective: Validate that an 837P Claims File (Adjusted Claim) is received, processed, accepted and an EDI 999 File (Implementation Acknowledgement) is generated and sent to Tellus eVV.

Test Scope: An 837P Claim File (Adjusted Claim) is received, processed, accepted and an EDI 999 File (Implementation Acknowledgement) responds with one of the following scenarios, 1) Accepted (no errors), 2) Accepted (with errors), or Rejected. If the 999 is Accepted with errors or Rejected, Payer's claims processing system responds with an EDI 835 (Health Care Claim Payment/Advice).

4.1.4.7. Claims Submission via 837P (Denied Claim Resubmitted) Completed by Tellus.

Prerequisite: Claim is in "Denied" status on the eVV Work List screen.

Objective: Validate that a resubmit claim transaction can be submitted and generate an 837P Claims File.

Test Scope: A Provider Administrator can "release" a resubmit claim. Status is displayed as RELEASED. The "Released" claim is processed and an 837P Claims file is generated and sent to Payer. Once the claim is processed, the claim status will display as SUBMITTED.

4.1.4.8. Claims Submission via 837P (Denied Claim Resubmitted) processed by Payer.

Prerequisite: Payer receives an 837P Claims File (Resubmit Claim).

Objective: Validate that an 837P Claims File (Resubmit Claim) is received, processed, accepted and an EDI 999 File (Implementation Acknowledgement) is generated and sent to Tellus eVV.

Test Scope: An 837P Claim File (Resubmit Claim) is received, processed, accepted and an EDI 999 File (Implementation Acknowledgement) responds with one of the following scenarios, 1) Accepted (no errors), 2) Accepted (with errors), or Rejected. If the 999 is Accepted with errors or Rejected, Payer's claims processing system responds with an EDI 835 (Health Care Claim Payment/Advice).

4.1.4.9. 999 Generated by Payer

Prerequisite: An 837P has been sent to Payer.

Objective: Validate that Payer has responded with valid 999 file.

Test Scope: Payer generates and transmits the following test cases:

1. An EDI 999 File is transmitted to Tellus with each of the following scenarios:
    1.1. Accepted (no errors).
    1.2. Accepted (with errors).
    1.3. Rejected.

4.1.4.10. 277 Generated by Payer

Note: Tellus does not machine-process the 277 file, this file is stored for reference during troubleshooting.

Prerequisite: An 837P has been sent to Payer, Payer has responded with a 999 Accepted (with errors) or 999 Rejected file.

Objective: Validate that Payer has responded with valid 277 file.

Test Scope: Payer generates and transmits a 277 file.

4.1.4.11. 835 (or 835-equivalent) Generated by Payer

Prerequisite: An 837P has been sent to Payer.

Objective: Validate that Payer has responded with a valid 835 or 835-equivalent files.

Test Scope: Payer generates and transmits the following test cases:

1. An EDI 835 (Health Care Claim Payment/Advice) is transmitted to Tellus and the claim status is set to each of the following:
   1.1. PAID.
   1.2. PAID PARTIAL.
   1.3. DENIED.

4.1.4.12. 999 Processed by Tellus

Prerequisite: An 837P has been sent to Payer and Payer has responded with a 999 file.

Objective: Validate that the Tellus eVV receives a 999, processes data and updates Tellus Claims status codes properly.

Test Scope: Tellus receives and processes the following test cases:

1. An EDI 999 File is transmitted to Tellus with each of the following scenarios:
   1.1. Accepted (no errors).
   1.2. Accepted (with errors).
   1.3. Rejected.

4.1.4.13. 835 Processed by Tellus

Prerequisite: An 837P has been sent to Payer and Payer has responded with 999 and 835 files.

Objective: Validate that the Tellus eVV receives and processes 835, processes data and updates Tellus Claims status codes properly.

Test Scope: Tellus receives and processes the following test cases:

1. An EDI 999 File is transmitted to Tellus with each of the following scenarios:
   1.1. Accepted (no errors).
   1.2. Accepted (with errors).
   1.3. Rejected.
2. An EDI 835 (Health Care Claim Payment/Advice) is transmitted to Tellus and the claim status is set to each of the following:
   2.1. PAID.

2.2. PAID PARTIAL.

2.3. DENIED.

4.1.5. VISIT MANAGEMENT TEST OBJECTIVES

4.1.5.1. Overnight Visit

Prerequisite: A visit that span two days (e.g., an overnight stay through midnight) has been completed.

Objective: Validate the processing of a single visit for services performed by the Caregiver that begins on one day and finishes on another (spanning two days).

Test Scope:

1. Review and release the claim in Tellus eVV Provider Portal.
2. Validate that 837P claim file for this visit generated and transmitted as expected and with the correct number of units and dollar amount calculation for the claim.

4.1.5.2. Multiple Recipients on a Single Visit – No TT Modifier

Prerequisite: A scheduled and completed visit with more than one recipient on a single visit.

Objective: Validate the processing of a single visit for services performed by the Caregiver for two or more recipients.

Test Scope:

1. Review and release the claim in Tellus eVV Provider Portal.
2. Validate that 837P claim file for this visit generated and transmitted as expected and with the correct number of units and dollar amount calculation for the claim.

4.1.5.3. Multiple Recipients on a Single Visit – TT Modifier

Prerequisite: A scheduled and completed visit with HCPCS/service code with TT modifier (multiple recipients with discounts) and more than one recipient on a single visit.

Objective: Validate the processing of a single visit for services performed by the Caregiver for two or more recipients with TT modifier.

Test Scope:

1. Review and release the claim in Tellus eVV Provider Portal.
2. Validate that 837P claim file for this visit generated and transmitted as expected and with the correct number of units and dollar amount calculation for the claim, including discounts.

4.1.5.4. Multiple Service codes on a single visit

Prerequisite: A scheduled and completed visit with HCPCS/service code with no TT modifier (multiple recipients with discounts) and more than one recipient on a single visit.

Objective: Validate the processing of a single visit for services performed by the Caregiver for two or more recipients with no TT modifier.

Test Scope:

1. Review and release the claim in Tellus eVV Provider Portal.
2. Validate that 837P claim file for this visit generated and transmitted as expected and with the correct number of units and dollar amount calculation for the claim, with no discounts.

4.1.5.5. GPS Maximum Range Between Scheduled and Actual Start

Prerequisite: Visits are scheduled in the eVV system

Objective: Validate that visits are started and completed within specified allowable range from the scheduled location and ensuing claim is generated and transmitted by Tellus.

Test Scope: Scheduled visits will be completed in range increments including exact address (zero variance), a location slightly less than the maximum range (.5 mile), a location equal to the maximum range, and a location out of range followed by submission of a claim.

4.1.5.6. Completed Late Visit

Prerequisite: Visits are scheduled in the eVV system

Objective: Validate visits after the scheduled start and finish times.

Test Scope: Scheduled visits will be completed beyond of scheduled time with the following scenarios, 1) Started on-time, finished late, 2) Started late, finished on-time, and 3) Started late, finished late. Verify that all scheduled and actual times are gathered as expected, and that ensuing claim is generated and transmitted by Tellus.

5. DEFECT MANAGEMENT

The criteria used to determine whether each test case has passed or failed will be based on conformance to the User Stories, Use Cases, and/or requirements. Test cases that produce an actual output not consistent with the expected results will be considered as failed and a defect report will be opened in Jira. Jira will be used to track progress of each defect as they are resolved and retested until closed.

6. APPROVALS

Tellus and Payer have reviewed and approve this test plan. This plan will be used as the plan for the Quality Assurance (QA) and User Acceptance Testing (UAT) cycles of the above-mentioned project.

Tellus Signature:	Name:	Date:
_____	_____	_____
Client Signature:	**Name:**	**Date:**
_____	_____	_____

-- The Tellus Team Looks Forward to Working with You --

7. APPENDIX A - ACRONYMS & DEFINITION OF TERMS

7.1. ACRONYMS

Table 5: Acronyms Used in this Document

Term	Definition/Description
277	Healthcare Claim Acknowledgement (Error Details)
835	Healthcare Claim Acknowledgement (Claim Payment and Remittance Advice)
837P	Standard Formatted Electronic Healthcare Claim
999	Healthcare Claim Acknowledgement (File received)
ACA	Affordable Care Act
ACHA	The Agency for Healthcare Administration
API	Application Program Interface
AWS	Amazon Web Services
EVV	Electronic Visit Verification
FIT	Feature Integration Test
FTP	File Transfer Protocol
GA	General Availability
HIPAA	Health Insurance Portability and Accountability Act
HITRUST	The Health Information Trust Alliance
HHA	Home Health Aide
HHS	U.S. Department of Health and Human Services
HRSA	Health Resources and Services Administration
JIRA	Agile project management and defect tracking software application
JSON	Lightweight data-interchange format for data object transmission
MIRTH	Cross-platform HL7 interface engine enabling bi-directional messages
PA	Prior Authorization
ePHI	Electronic Protected Health Information
POS	Point of Service
PSD	Product Specification Document
SCM	Software Configuration Management
SVT	System Validation Test
TCS	Test Case Specification
TDS	Test Design Specification

7.2. DEFINITION OF TERMS

21st Century Cures Act	United States law enacted in December 2016 to accelerate the discovery, development, and delivery of 21st century cures, and for other purposes.
Acceptance Testing	Testing conducted to determine if the minimal requirements and/or specifications have been met and the product is ready for release.
Black-box Testing	Testing derived from a functional design specification without regard to the internal program structure and executed via end user or external interfaces.
Browser Compatibility Testing	Testing conducted to evaluate if an application or system works using different browsers.
Entrance Criteria	Metrics specifying the condition that must be met to begin testing at the next stage, phase, or level.
Exit Criteria	Metrics specifying the condition that must be met to promote a product or work unit to the next stage, phase, or level.
Exploratory Testing	Testing not derived specifically from a functional design specification but is executed via end user or external interfaces.
Functional Testing	Process of testing to verify that the functions of a system are present and operate as specified; testing from a block-box perspective. *Also known as Feature Testing*
Hardening Cycle	An additional sprint added for the purpose of executing Regression Testing, Bug Validation/Fixing, and specialty testing such as Security, Compliance, User Acceptance, prior to final release to production.
Production Environment	The environment where your system and services are made available to your customers.
Regression Testing	Testing that exercises a comprehensive set of test cases intended to verify that the system properly functions without degradation after changes have been applied.
Staging Environment	An environment that is a nearly exact replica of a production environment used for final updates and validation

	testing to assure the system is ready for Production. *Also known as UAT Environment.*
Stress Testing	Testing in which a system is subjected to unlikely or unrealistically harsh inputs (over loaded) or loaded with inadequate resources with the intention of identifying system limitations.
Structural Testing	Process of testing the consistency of a component's implementation with its design; testing from a white-box perspective
System Test	Testing to verify the product's integrated software, hardware, and documentation to the functional and operational requirements.
Visit	The act of performing a scheduled service by a trained caregiver.
White-box Testing	Testing derived from an internal design specification and/or the code and executed with knowledge of the internal program structure. *Also known as Clear-box Testing*

TELLUS

POL – 0EXE - 08
CHANGE CONTROL

Table of Contents

REVISION TABLE 2
PURPOSE 3
CONFIDENTIALITY, INTEGRITY AND AVAILABILITY 3
SCOPE 3
ACRONYMS AND DEFINITIONS 3
RESPONSIBILITIES 5
POLICY 5
Program Implementation 5
Change Management Board 5
Required Procedures 5
Upgrade Guidelines 7
No longer supported systems 7
Environmental Separation 8
Environments 8
Development (Dev) 8
Quality Assurance (QA) 9
Staging (STG) 10
User Acceptance Testing (UAT) 11
Production (Prod) 11
Operational Issue Prevention 12
REFERENCES 13

REVISION TABLE

Date	Description	Revised By	CCR #	Version
23 April 2018	Initial	Michael B. Morell, CISSP	A2TCS-26	.00
20 June 2018	Addition of Staging	Michael B. Morell, CISSP	A2TCS-26	.01
25 July 2018	Reviewed and approved	Michael B. Morell, CISSP	A2TCS-26	1.0
11 Aug 2018	Added C.I.A.	Michael B. Morell, CISSP	A2TCS-155	1.1
15 Aug 2018	Added Sub-Contractors	Michael B. Morell, CISSP	A2TCS-139	1.2
28 Sep 2018	Ready for Approval	Michael B. Morell, CISSP	A2TCS-26	1.3

PURPOSE

The purpose of this Policy is to give guidance on the Companies Change Control Program.

CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

This Policy shall demonstrate a clear commitment to maintaining and enforcing Confidentiality, Integrity, and Availability of Protected Health Information, Personally Identifiable Information and Non Public Personal Information.

SCOPE

Tellus has a commitment to maintaining and enforcing confidentiality, integrity, and availability of PHI.

The scope of this policy shall include the following areas:

1. Program Implementation
2. Change Control Board
3. Required Procedures
4. Environmental Separation

This policy applies to all Company employees, contractors, sub-contractors, consultants, temporary and other workers, and all third-party service personnel who access the Company network.

ACRONYMS AND DEFINITIONS

CCB – Change Control Board.

Company – This refers to Tellus, LLC Company as an entity.

DSO - Designated Security Officer. This person shall be designated by the CEO and identified as such in the organizational chart by the three (3) letter designation by their name.

Employee – unless otherwise stated, employee may mean any staff member of the company to include, full and part time employees, contractors, agents, and third parties acting on behalf of the company.

SCM – Software Configuration Management Team

RESPONSIBILITIES

1. The CEO is ultimately responsible for this policy and its approval.

2. The DSO is responsible for all changes, reviews, and updates to this policy. Reviews shall occur on a yearly basis.

3. The DSO is responsible for the creation of a Change Control Board.

4. The Change Management Board is responsible for the procedures required to enact changes and to give guidance on this Policy.

POLICY

Program Implementation

The Company shall institute a common change management program that shall be used across all departments.

Change Management Board

The DSO will create and oversee the Change Control Board (CCB). Each Department shall have a representative on the CCB.

Required Procedures

The CCB shall create procedures for the following items:

1. The manner of identifying and recording of significant changes.

2. The planning and testing of changes

3. Conduct the assessment of the potential impacts, including security impacts, of such changes.

    a. The system owner shall provide evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times.

b. This process shall include a risk assessment, analysis of the security and privacy impacts of changes, and specification of security controls needed. This process shall also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained.

4. Establish the formal approval of proposed changes.

5. Establish the communication of change details to all relevant persons

6. Ensure that as part of all change controls, that fallback procedures be defined and implemented, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.

7. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management

8. Establishes a process for identifying configuration items throughout the system development life cycle, and for managing the configuration of the configuration items.

9. Acceptance of new systems is clearly defined, agreed, documented and tested.

10. Perform unit, integration, system and regression testing/evaluation in accordance with organization-defined requirements for depth and coverage

11. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation

12. Implement a verifiable flaw remediation process.

    a. Correct flaws identified during security testing/evaluation.

    b. The Company shall require the developer of the information system, system component, or information system service to track security flaws and flaw resolution within the system, component, or service and report findings to Company-defined personnel or roles.

13. Ensure that a rollback strategy is in place before changes are implemented. Rollback procedures shall include backups of all relevant data that is being changed.

14. Rules for the migration of software from development to operational status shall be defined and documented by the Company hosting the affected application(s), including that development, test, and operational systems be separated (physically or virtually) to reduce the risks of unauthorized access or changes to the operational system.

Upgrade Guidelines

Any decision to upgrade to a new release shall take into account the business requirements for the change, and the security and privacy impacts of the release (e.g., the introduction of new security functionality or the number and severity of security problems affecting this version).

Prior to any changes to a Production environment, a current backup of all relevant data shall be conducted. Previous versions of application software shall be retained as a contingency measure. Old versions of software shall be archived, together with all required information and parameters, procedures, configuration details, and supporting software for as long as the data is retained in archive or as dictated by the company's data retention policy.

No longer supported systems

If systems or system components in production are no longer supported by the developer, vendor, or manufacturer, the Company must show evidence of a formal migration plan approved by management to replace the system or system components.

Environmental Separation

As part of the Change Control process, unique environments shall be maintained. The Change Control process will strive to create an environment that minimizes any testing on production systems. When testing must be performed, a test plan shall be developed that documents all changes to the system and the procedures for undoing any changes made to the system

Environments

Development (Dev)

The Dev environment is where all code is originated and initially tested. This environment access controls are controlled by the SCM team, while all code source is operated by the Dev team. The Development team Manager shall have final authority over what dev team members may access parts of source code or dev servers.

No Production data may be used or stored in Dev.

If covered, or otherwise sensitive, information must be used for testing purposes, all sensitive details and content shall be removed or modified beyond recognition (e.g., de-identified) before use.

The following requirements shall be applied to protect data, when used for testing purposes:

1. The access control procedures, which apply to operational application systems, shall also apply to test application systems.

2. There shall be formal management authorization for instances where operational information is copied to a non-production application system.

3. Operational information and test accounts shall be erased from a test application system immediately after the testing is complete.

Quality Assurance (QA)

The QA environment is the first environment that resembles Production, and where code may be tested, that will be simulating Production.

Environment Access shall be limited to those individuals that are required to perform QA activities. Code deployments to this environment shall require a change control but does not require CCB approval. In order to test instruction accuracy, code deployments into QA will be performed by both the SCM and Dev Team member.

No Production data may be stored or used in QA.

If covered, or otherwise sensitive, information must be used for testing purposes, all sensitive details and content shall be removed or modified beyond recognition (e.g., de-identified) before use.

The following requirements shall be applied to protect data, when used for testing purposes:

1. The access control procedures, which apply to operational application systems, shall also apply to test application systems.

2. There shall be formal management authorization for instances where operational information is copied to a non-production application system.

Operational information and test accounts shall be erased from a test application system immediately after the testing is complete.

Staging (STG)

The STG environment is where demos and training of the application are done. This environment is semi open, requiring username and passwords to enter, but is not restricted to solely customers and end users.

The STG environment shall closely resemble Production.

No Production data may be stored or used in STG.

Only test data may be used in STG. Any information entered into a STG system, must be fictitious.

Special note about user accounts

For applications such as demo sites, where the sales team are presenting the application to potential customers, it is preferred that unique usernames and password be generated for the customer.

The username and password for the demo portion of the environment may be generic while remaining unique to the customer. All such demo accounts will be deemed temporary and must be removed or deactivated within 48 hours of the presentation being concluded.

Training accounts shall be issued on a per user basis and shall be enabled for 30 days. After 30 days, a training account shall be automatically disabled.

User Acceptance Testing (UAT)

The UAT environment is where end users of the application can validate that the changes behave as expected. UAT environment access shall be restricted to only customers and end users that require access. When at all possible, the UAT environment shall not be made public.

The UAT environment shall closely resemble Production.

No Production data may be stored or used in UAT.

If covered, or otherwise sensitive, information must be used for testing purposes, all sensitive details and content shall be removed or modified beyond recognition (e.g., de-identified) before use.

The following requirements shall be applied to protect data, when used for testing purposes:

1. The access control procedures, which apply to operational application systems, shall also apply to test application systems.

2. There shall be formal management authorization for instances where operational information is copied to a non-production application system.

Operational information and test accounts shall be erased from a test application system immediately after the testing is complete.

Production (Prod)

Production environments consist of any architecture where its outage will have monetary loss or a loss of customer confidence. The following regions are considered to be Production:

1. Any Network Infrastructure where its outage would bring down any customer or internal systems.

2. Any Customer facing Server (web, database, application) that holds or processes production data.

Operational Issue Prevention

The level of separation between Dev, QA, UAT and Production environments shall be identified, with controls implemented to prevent operational issues.

Such controls shall include.

1. A review of all custom code preceding the release to production or to customers must be completed in order to identify any possible coding vulnerability.

2. Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices

3. Code reviews ensure code is developed according to secure coding guidelines.

4. Code-review results are reviewed and approved by management prior to release

5. Appropriate corrections to code are implemented prior to release to Production.

6. Develop, document, and maintain under configuration control, a current baseline configuration of the information system. The Company shall review and update the baseline configuration of the information system:

    a. at least once every six (6) months

    b. when required due to critical security patches, upgrades and emergency changes (e.g., unscheduled changes, system crashes, replacement of critical hardware components), major system changes/upgrades.

    c. as an integral part of information system component installations or upgrades.

    d. Supporting baseline configuration documentation reflects ongoing implementation of operational configuration baseline updates, either directly or by policy.

7. Any issues discovered in the in any environment must go thru all environmental level testing. For example. If an issue is discovered in UAT, it must be fixed in Dev and then tested in QA before deployment to UAT.

8. Prior to deploying to the Prod environment, all known bugs must be addressed in the lower environments.

9. Test data and accounts shall be removed completely before the application is placed into a production state.

10. All custom application accounts, user IDs, and passwords, shall be removed before applications go from development to production or are released to customer.

11. Development and operational software shall run on different systems with logical boundaries. Eg no development system can be on a production network/vlan.

12. Compilers, editors, and other development tools or system utilities shall not be accessible from QA, UAT or Production systems when not required.

13. The test system environments shall emulate the Production environment as closely as possible.

14. Unique Services accounts shall be created for each environment. No Dev, QA or UAT service accounts are allowed to be used in Production.

15. Users shall use different user profiles for operational and test systems, and menus shall display appropriate identification messages to reduce the risk of error.

REFERENCES

1. POL-0EXE-01-SecurityPolicy
2. POL-0MRK-01-CommunicationAndInformationDisclosure

TELLUS

POL – 0EXE - 02
RISK MANAGEMENT PROGRAM

Table of Contents

REVISION TABLE 3
PURPOSE 3
CONFIDENTIALITY, INTEGRITY AND AVAILABILITY 3
SCOPE 4
ACRONYMS AND DEFINITIONS 4
RESPONSIBILITIES 5
POLICY 5
Risk Management Program Areas 5
Phase 1: Risk Assessment 5
Phase 2: Business Continuity Planning 5
Phase 3: Disaster Recovery Planning 5
Risk Management Discovery Areas 6
Discovery Areas 6
Risk Criteria 8
Risk Analysis 10
Conducting a Risk Analysis 10
Vulnerability Assessments 11
Inclusion of risk areas 12
Permanent Risk Areas 12
Removal of risk areas 14
Defining Risk 15
Authorization of suspension of a Risk Analysis 15
Risk Report 15
Identified Risk Area Remediation 16
High Risk Systems 16
Disaster Recovery Sites 16
BCP and DR Concepts 17
BCP and DR Testing 18
Customer Specific BCP and DR planning 19
Service Providers 19
REFERENCES 20

REVISION TABLE

Date	Description	Revised By	CCR #	Version
23 April 2018	Initial	Michael B. Morell, CISSP	A2TCS-15	.00
11 Aug 2018	Added C.I.A.	Michael B. Morell, CISSP	A2TCS-155	.01
15 Aug 2018	Added Sub-Contractors	Michael B. Morell, CISSP	A2TCS-139	.02
28 Sep 2018	Approval	Michael B. Morell, CISSP	A2TCS-15	1.0

PURPOSE

This Company Risk Management Program, which includes Risk Assessment, Business Continuity Planning and Disaster Recovery Test Scripts, is intended to give define the role that Risk Management plays within the company.

The Risk Management Program provides the company with a framework in which to assess the various risks associated with doing business in its present form. The risk analysis framework is meant to serve as a guide to the assessor as to the procedures that are needed to be followed in order to complete an accurate assessment.

A formal Risk Analysis is meant to be prepared yearly and presented to Executive Management as well as the Board of Directors. The reports assessment is meant to guide the company to both resolving issues that it may or may not be aware of as well as serve as the foundation for the BCP/DR programs.

This program overview document is classified as Internal Use Only and may not be transmitted to third parties and clients with their solution specific plans.

For transmittal to third parties, please use POL-0EXE-03-RiskManagementProgramOverview

CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

This Policy shall demonstrate a clear commitment to maintaining and enforcing Confidentiality, Integrity, and Availability of Protected Health Information, Personally Identifiable Information and Non Public Personal Information.

SCOPE

Tellus has a commitment to maintaining and enforcing confidentiality, integrity, and availability of PHI.

The scope of the risk management program shall be based upon the Australian/New Zealand Standard "AS/NZS 4360:2004 Risk Management".

Utilizing the standard, this policy will define the following areas:

1. Risk Management Program Areas
2. Risk Management Discovery Areas
3. Risk Criteria
4. Risk Analysis
5. BCP and DR Concepts
6. Customer Specific BCP and DR planning
7. Service Providers

This policy applies to all Company employees, contractors, sub-contractors, consultants, temporary and other workers, and all third-party service personnel who access the Company network.

ACRONYMS AND DEFINITIONS

BCP - Business Continuity Planning. Business continuity planning involves assessing the risks to organizational processes and creating policies, plans, and procedures to minimize the impact those risks might have on the organization if they were to occur. BCP is used to maintain the continuous operation of a business in the event of an emergency situation. BCP is the foundation of the plan.

Company – This refers to Tellus, LLC company as an entity.

DSO - Designated Security Officer. This person shall be designated by the CEO and identified as such in the organizational chart by the three letter designation by their name.

Employee – unless otherwise stated, employee may mean any staff member of the company to include, full and part time employees, contractors, agents, and third parties acting on behalf of the company.

PII – Personally Identifiable Information

NPI – Non Public Information

PHI – Protected Health Information

RESPONSIBILITIES

1. The CEO is ultimately responsible for this policy and its approval.

2. The DSO is responsible for implementing the DR and BCP programs

3. Client Relationship Managers are responsible for ensuring that their customers have DR and BCP programs enacted for their solution.

POLICY

Risk Management Program Areas

The Risk Management Program consists of three areas: Risk Assessment, Business Continuity Planning and Disaster Recovery Test Scripts. All three areas have natural overlap.

Phase 1: Risk Assessment

In this phase, a Risk Assessment is performed against either company assets or a customer solution. Based on the information found in the Risk Assessment, a Business Continuity Plan is built.

Phase 2: Business Continuity Planning

In the BCP Phase, likely real world scenarios are applied to the various risk areas. "Likely" real world scenarios are preferred over "hypothetical" scenarios and garner a more realistic approach to developing a plan. The results that are found in this stage lay the foundation for the DR test scripts.

Phase 3: Disaster Recovery Planning

In this last phase, scripts are written that serve two purposes:

1. They can be used as a script to conduct controlled failure tests.

2. They can be used as a plan when an unexpected failure occurs.

The results of DR test scripts are typically, what are included with Audits and customer requests for BCP/DR plans.

Risk Management Discovery Areas

Utilizing RMP-0EXE-06-RiskAnalysis, pre-defined areas that require a risk analysis shall be maintained. The following is a general list and may be expanded on the risk analysis form without requiring update and approval to this policy. Removal of any items from this list will require an update and approval to this policy.

Discovery Areas

1. General
   This section of the Risk Analysis will define all of the stakeholders and establish the context of the objectives.

   a. Primary and Secondary Assessors shall be identified. The assessor is the individual responsible for conducting the Risk Assessment. The Assessor may be an internal resource or a 3rd party auditor.

   b. Stakeholders shall be identified for each division of the company. A stakeholder or 'responder', will be the individual(s) responsible for answering to the assessor, their areas of governance. A stakeholder may be assigned multiple areas of governance or may be secondary responders to a given risk area.

   c. Context Establishment is important in order to ensure that the objectives defined for the risk management process take into account the organizational and external environment.

      i. At the beginning of each new Risk Analysis primary objective will be defined. This will provide the overall direction for the risk analysis, as each year the objective may change.

      ii. In addition to a primary objective, a secondary objective may also be defined. This may be a complimentary objective to the primary.

      iii. The defining of any ancillary objectives shall also be included. Unlike Primary and Secondary objects, ancillary objectives do not have a direct impact on the overall direction, but are information that would help with the overall assessment.

2. Corporate Systems
   This section is used to define Corporate specific systems that can impact the overall company work flow. Items may be:
   a. Domain Controllers
   b. Mail Servers
   c. PBX systems
   d. File Servers
   e. Development Systems
   f. End users switches
   g. Internal Name Servers

3. Shared Infrastructure
   Shared Infrastructure is defined as items that are not expressly used for just company or client access. Items may be:

   a. Firewalls
   b. Load Balancers
   c. Database Servers
      i. Production
      ii. UAT
      iii. QA
   d. Web Servers
   e. FTP Servers
   f. External Name Servers

4. Staffing
   In the staffing section, define the critical positions required to maintain the core efficiency of each department.

5. Security
   Review the following areas:

   a. Information Security Program
   b. Third Party Agreements
   c. Change Management Procedures

6. Procedures and Best Practices
   A review of all key systems should be made as to their operating procedures and best practices that are applied.