



The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

Header 4

[List View](#)

General Information [Contact](#) [Default Values](#) [Discount](#) [Document Information](#) [Clarification Request](#)

Procurement Folder: 845238

SO Doc Code: CRFQ

Procurement Type: Central Contract - Fixed Amt

SO Dept: 0506

Vendor ID: VS0000008715

SO Doc ID: BHS2100000003

Legal Name: FEI.COM, INC.

Published Date: 4/1/21

Alias/DBA:

Close Date: 4/13/21

Total Bid: \$1,543,926.00

Close Time: 13:30

Response Date: 04/13/2021

Status: Closed

Response Time: 12:11

Solicitation Description: WEB-BASED DATA COLLECTION SYSTEM

Responded By User ID: jennifer.conrad

Total of Header Attachments: 4

First Name: Corey

Total of All Attachments: 4

Last Name: Atanda

Email: corey.atanda@feisystem

Phone: 908-635-9218



Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder: 845238
Solicitation Description: WEB-BASED DATA COLLECTION SYSTEM
Proc Type: Central Contract - Fixed Amt

Solicitation Closes	Solicitation Response	Version
2021-04-13 13:30	SR 0506 ESR04132100000007012	1

VENDOR
VS0000008715
FEI.COM, INC.

Solicitation Number: CRFQ 0506 BHS2100000003
Total Bid: 1543926
Response Date: 2021-04-13
Response Time: 12:11:31
Comments:

FOR INFORMATION CONTACT THE BUYER
Crystal G Hustead
(304) 558-2402
crystal.g.hustead@wv.gov

Vendor		
Signature X	FEIN#	DATE

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Business function specific software				484119.00

Comm Code	Manufacturer	Specification	Model #
43231500			

Commodity Line Comments: System configuration for SOR, ASAM, Waitlist and Prevention. Tier 3 support and hosting for 2 months; training for all features other than Prevention.

Extended Description:

Web-Based Data Collection System Software with capability to collect all SAMHSA required GPRA data and submit data to SPARS nightly.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Renewal 1				385137.00

Comm Code	Manufacturer	Specification	Model #
43231500			

Commodity Line Comments: Prevention Training. One year 525 CONTINUUM subscriptions; one year 40 CO-Triage Subscriptions, for period ending 9/29/2022. Tier 3 support; hosting; clinical support from ASAM.

Extended Description:

Renewal 1

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Renewal 2				337335.00

Comm Code	Manufacturer	Specification	Model #
43231500			

Commodity Line Comments: One year 525 CONTINUUM subscriptions; one year 40 CO-Triage Subscriptions. Tier 3 support; hosting; clinical support from ASAM.

Extended Description:

Renewal 2

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Renewal 3				337335.00

Comm Code	Manufacturer	Specification	Model #
43231500			

Commodity Line Comments: One year 525 CONTINUUM subscriptions; one year 40 CO-Triage Subscriptions. Tier 3 support; hosting; clinical support from ASAM.

Extended Description:

Renewal 3

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ BHS2100000003

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:

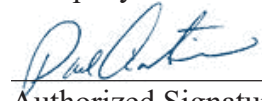
(Check the box next to each addendum received)

- | | |
|--|--|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6 |
| <input type="checkbox"/> Addendum No. 2 | <input type="checkbox"/> Addendum No. 7 |
| <input type="checkbox"/> Addendum No. 3 | <input type="checkbox"/> Addendum No. 8 |
| <input type="checkbox"/> Addendum No. 4 | <input type="checkbox"/> Addendum No. 9 |
| <input type="checkbox"/> Addendum No. 5 | <input type="checkbox"/> 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 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.

FEI.com, Inc. dba FEI Systems (FEI)

Company



Authorized Signature

April 12, 2021

Date

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

STATE OF WEST VIRGINIA
West Virginia Department of Health and Human Resources,
Bureau for Behavioral Health

Web-Based Data Collection System

CRFQ BHS2100000003

Response prepared by FEI Systems

Submitted to Ms. Crystal Hustead

April 13, 2021

West Virginia Department of Health and Human Resources, Bureau for Behavioral Health
Web-Based Data Collection System

CRFQ BHS2100000003

Prime Contractor Submission:

FEI.com, Inc. dba FEI Systems

9755 Patuxent Woods Drive, Suite 300 | Columbia, Maryland 21046 | (443) 270-5100

Authorized Negotiator:

Dave Castille, President

(443) 270-5127 | Dave.Castille@FEISystems.com

Additional Points of Contact:

Jennifer Conrad, Vice President, Behavioral Health Business

(443) 270-5148 | Jennifer.Conrad@FEISystems.com

Corey Atanda, Business Development Executive

(908) 635-9218 | Corey.Atanda@FEISystems.com

DUNS: 160886888 | TIN: 52-2067447

Table of Contents

Acronym List.....	iii
Transmittal Letter.....	iv
1 Executive Summary	1
2 Mandatory Requirements [CRFQ 4]	3
2.1 Mandatory Contract Services Requirements and Deliverables [CRFQ 4.1].....	3
2.2 Standards of Privacy and Security [CRFQ 4.2].....	8
2.3 Deliverables, Scope of Work, and Timeframe [CRFQ 4.3]	20
2.3.1 Deliverable 1: ASAM CONTINUUM™ and CO-Triage® Integration [CRFQ 4.3.2]	20
2.3.2 Deliverable 2: Statewide Bed Waitlist and Management Module [CRFQ 4.3.3]	21
2.3.3 Deliverable 3: State Opioid Response (SOR) Grant GPRA Reporting Module [CRFQ 4.3.4]	25
2.3.4 Deliverable 4: Prevention Module [CRFQ 4.3.5]	29
2.3.5 Deliverable 5: User and Administrative/Technical Manuals [CRFQ 4.3.6].....	31
2.3.6 Deliverable 6: Training [CRFQ 4.3.7]	32
2.3.7 Maintenance, Support, and Upgrades [CRFQ 4.3.8]	33
3 Miscellaneous – Contract Manager [CRFQ 9; CRFQ 9.1].....	38

List of Exhibits

Exhibit 1. FEI Qualifications [CRFQ 3]	2
Exhibit 2. Grants Management Dashboard	4
Exhibit 3. Client Consent Form Page.....	5
Exhibit 4. Sample Prevention Block Grant Report from SSRS.....	7
Exhibit 5. Controls Hierarchy and Inheritance Structure	9
Exhibit 6. WITS Issue Severity Matrix Ensures	19
Exhibit 7. Help Desk work items are addressed quickly based on WITS standard SLAs	19
Exhibit 8. Filtered List of Programs with Open Beds	22
Exhibit 9. List of Clients Waiting for a Program	22
Exhibit 10. ASAM CONTINUUM Level of Care Recommendation	23
Exhibit 11. Client Service Authorization.....	23
Exhibit 12. Client Waitlist Profile captures required timeliness reporting data	24
Exhibit 13. Program Set Up Screen Shows Grant, Level of Care and Evidence Based Practices	26
Exhibit 14. Client Activity List is tied to Client’s Profile information	27
Exhibit 15. WITS Prevention Features follow the SPF Model.....	29
Exhibit 16. Planned Training Sessions	33
Exhibit 17. SolarWinds Sample Report	34
Exhibit 18. Help Resources File Upload Window.....	37
Exhibit 19. FEI Hosting Redundancy Approach Promotes System Availability.....	37

Acronym List

Acronym	Definition
ASAM	American Society for Addiction Medicine
ASI	Addiction Severity Index
BBH	Bureau for Behavioral Health
BHSIS	Behavioral Health Services Information System
CDSS	Clinical Decision Support System
CFR	Code of Federal Regulations
CRFQ	Centralized Request for Quote
CSAP	Center for Substance Abuse Prevention
CSF	Common Security Framework
FEI	FEI.com, Inc. dba FEI Systems
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FoD	Fortify on Demand
GPRA	Government Performance and Results Act
HIPAA	Health Insurance Portability and Accountability Act
HITRUST	Health Information Trust Alliance
ICD	Interface Control Document
IRT	Incident Response Team
ISO	International Organization for Standardization
IOM	Institute of Medicine
IT	Information technology
NOMs	National Outcome Measures
PHI	Protected Health Information
PII	Personally Identifiable Information
PRISM	Privacy, Risk, & Information Security Management
SAIS	Services Accountability Improvement System
SAMHSA	Substance Abuse and Mental Health Services Administration
SAPT	Substance Abuse Prevention and Treatment
SAST	Static Application Security Tests
SBIRT	Screening, Brief Intervention, and Referral to Treatment
SCCM	System Center Configuration Manager
SPF	Strategic Prevention Framework
SLA	Service Level Agreement
SOR	State Opioid Response
SPARS	SAMHSA Performance Accounts ability and Reporting System
SQL	Structured Query Language
SSO	Single Sign-On
SSRS	SQL Server Reporting Services
SUD	Substance Use Disorder
TEDS	Treatment Episode Data Set
TSC	Tenable Security Center
TRAC	Transformation Accountability
URS	Uniform Reporting System
WebBGAS	Web Block Grant Application System
WITS	Web Infrastructure for Treatment Services
WVDHHR	West Virginia Department of Health and Human Resources

Transmittal Letter

April 13, 2021

Ms. Crystal Hustead
West Virginia Department of Health and Human Resources, Bureau for Behavioral Health
2019 Washington Street, East
Charleston, West Virginia 25305

Dear Ms. Hustead:

FEI.com, Inc. dba FEI Systems (FEI) provides innovative behavioral health case management information technology solutions that assist federal, state, and local agencies in providing high quality, compassionate mental health treatment services. With extensive experience and deep subject matter expertise, FEI is uniquely qualified to partner with the West Virginia Department of Health and Human Resources, Bureau for Behavioral Health in the development and implementation of a **Web-Based Data Collection System, and we are pleased to submit our response to Centralized Request for Quote (CRFQ) BHS2100000003**. FEI meets all the mandatory requirements of this solicitation.

FEI acknowledges the receipt of this solicitation and Amendment #1, dated April 1, 2021. Our proposal remains valid for 180 days.

Please contact me at (443) 270-5127 should you have any questions or require any additional information. We appreciate this opportunity and look forward to working with West Virginia Department of Health and Human Resources, Bureau for Behavioral Health.

Sincerely,



Dave Castille
President

1 Executive Summary

Since 2003, FEI.com, Inc. dba FEI Systems (FEI) has provided our Web Infrastructure for Treatment Services (WITS) Platform to state and county agencies, with the primary objective of providing them with access to a system that is not only compliant with the Substance Abuse and Mental Health Services Administration's (SAMHSA) reporting requirements but also supports the workflow needs of their contracted provider communities. We have been actively distributing the American Society for Addiction Medicine (ASAM) products to states for more than two years and have been ASAM's partner to develop and modify the software since 2013. Our platform meets all of the State's requirements, including:

1. FEI is an authorized distributor of ASAM CONTINUUM and ASAM CO-Triage.
2. FEI has been developing software for states, counties, and the federal government to support the State Opioid Response (SOR) grant, Prevention and Treatment Block grants, and Treatment Episode Data Set (TEDS)/National Outcome Measures (NOMs) data collection, since 2000.
3. FEI has been providing systems for states that capture, store, and upload Government Performance and Results Act (GPRA) data since 2007, first to Services Accountability Improvement System (SAIS), and then to SAMHSA's new platform, SAMHSA Performance Accounts Ability and Reporting System (SPARS).
4. FEI has been supporting 42 Code Federal Regulations (CFR) part 2 compliant consent and referrals since 2003 for states, counties, and providers; and has been supporting 1115 waiver implementations since 2013.

An enterprise-level solution, WITS naturally segments data by provider agency, which ensures that each treatment or prevention provider agency the state establishes will see only its own data in the system.

Originally built under SAMHSA's direction, WITS includes data collection workflows for substance abuse and mental health TEDS/NOMs, along with a structured file format that states can use for submission to the Behavioral Health Services Information System (BHSIS). While the original system supported substance abuse treatment block grant data collection and reporting, several customers have added features to include mental health block grant and Uniform Reporting System (URS) reporting. Integration with the ASAM CONTINUUM engine and its associated assessment modules have also been added. Many states and counties now use a full state-wide waitlist to manage their scarce treatment resources and ensure patients with priorities (such as pregnancy, HIV, IV drug use, or other state-determined priorities) are given the first advantage when beds or slots become available. Both the ASAM integration and state-wide waitlist have been key features in our support of states and counties pursuing the 1115 waiver for Substance Use Disorder (SUD) in their communities.

The original WITS platform also included a 42 Code of Federal Regulations (CFR) part 2 compliant consent and referral module for sharing of data between providers. This has become an integral part of the system for care delivery, allowing for coordination of clinical records between various provider agencies within a state and continuity of a grant-related episode to support SAMHSA's GPRA reporting requirements. This module is also used as part of the state-wide waitlist feature, so data from one provider can be shared with a receiving provider when a bed or slot becomes available.

In partnership with several state customers, FEI designed and structured a prevention reporting system that follows the Strategic Prevention Framework model. It supports community-based assessments, which can be tied to regional or state-wide plans, allows for both community-based and individual-based implementation data capture that is tied back to the plans, records planned and actual costs, and facilitates all block grant and other Center for Substance Abuse Prevention (CSAP) required reporting. In

addition, this module can be used for other types of prevention such as suicide and tobacco/smoking and employed for training and technical assistance planning across the state.

WITS modules were also designed with state and provider reporting in mind. Each WITS implementation has an easy-to-use reporting module, which currently uses Microsoft's Structured Query Language (SQL) Server Reporting Services (SSRS) feature. This allows the State and its designated providers to build, manage, and run reports on any data within the database—allowing for ad-hoc queries posed by the legislature, or for deep analysis and evaluation of trends within the treatment and prevention infrastructure of the State. Reporting is available in real time against the system data and is accessed based on permissions through a single sign-on (SSO) to the platform.

Our commitment to covering the SAMHSA reporting requirements for states began in 2000 when FEI worked under SAMHSA contract to design and build the first iteration of the WITS platform. Since then, we have continued to contract with SAMHSA, building the SAIS and Transformation Accountability (TRAC), and later providing all the software support to merge the features into SPARS. Since 2010, FEI has managed/supported SAMHSA's Web Block Grant Application System (WebBGAS) system. More importantly, we have maintained partnerships with our customers across the US to improve and grow the capabilities of the system, to respond to new requirements, and to collaboratively share reporting, program, and system ideas.

As shown in **Exhibit 1**, FEI and our staff have the qualifications to perform this work as required by this solicitation.

Exhibit 1. FEI Qualifications [CRFQ 3]

Requirement	Proof Point(s)
American Society for Addiction Medicine (ASAM) authorized distributor of ASAM CONTINUUM™ and ASAM CO-Triage® [CRFQ 3.1]	FEI is an authorized distributor of ASAM CONTINUUM and ASAM CO-Triage and has been supporting states and counties, as well as providers, who use these tools, since 2018.
Minimum two years of experience working with ASAM on ASAM CONTINUUM and ASAM CO-Triage [CRFQ 3.2]	Since 2013, FEI has partnered with ASAM to build the ASAM CONTINUUM assessment platform and continues to maintain the site as well as program and test all modifications to these tools for ASAM.
Minimum two years of experience developing software systems that capture and report data for the federal SAMHSA State Opioid Response grant and SAMHSA Substance Abuse Prevention and Treatment (SAPT) and Community Mental Health Block Grants. Vendor will transfer TEDs data in a format approved by BBH/MIS [CRFQ 3.3]	FEI first introduced WITS to states and counties in 2003, capturing all data required for the treatment block grant reporting, as well as TEDS data collection. In 2009, FEI added prevention and mental health block grant data. The majority of FEI's 37 WITS customers report this data directly from the system, including a formatted TEDS data upload that the state can send directly to BHSIS. In addition, FEI has supported the WebBGAS system for SAMHSA since 2010.
Minimum of two years of experience developing software systems that capture and store federal Government Performance and Results Act (GPRA) data and upload data into the SAMHSA Performance Accounts Ability and Reporting System (SPARS) [CRFQ 3.4]	FEI has been helping states and other grantees with the collection, storage, and reporting of the CSAT GPRAs since 2007, and has supported more than 75 grants since that time. These were originally reported to SAIS but are now directly uploaded nightly to SPARS. In addition, FEI is the company that provided the majority of the programming for SPARS.
Two years of experience developing software systems that capture and report data regarding the Medicaid	Since 2003, WITS has included a 42 CFR part 2 compliant consent process; and since 2018 FEI has assisted states

Requirement	Proof Point(s)
1115 Waiver and 42 CFR Part 2 consent and referrals [CRFQ 3.4]	and counties in their implementation of the Medicaid 1115 SUD Waiver.

2 Mandatory Requirements [CRFQ 4]

2.1 Mandatory Contract Services Requirements and Deliverables [CRFQ 4.1]

- *Software and Integration Requirements for Web-Based Data Collection System. Software must track and allow users access to data and information appropriate to their access level. [CRFQ 4.1.1]*

Our proposed Data Collection System, WITS, is a modular, web-based application designed to meet the growing need to capture client services data, including outcomes and costs, in one centralized place. WITS serves more than 37 states and counties across the US, with data reporting in from close to 10,000 provider agencies nationwide. Each state or county has its own implementation of the WITS system. While many of the key reporting features and database structures are consistent across most customers, each customer's instance is configured to meet its specific needs. Each customer can also manage its provider agencies, staff, and the wide variety of programs that will be reported upon within the system. This provides the ability to manage the access that various users have to portions of the system, and limit access based on each user's unique roles and needs.

WITS was originally conceived by SAMHSA as a web-based system for states to submit required Substance Abuse treatment block grant data as well as the TEDS/ NOMs data to the federal government. However, it was designed to include a workflow-driven tool to support clinical practices for timely and accurate data collection. As the number of states and counties using WITS increased, they began working with FEI to add features such as Prevention, billing, court and forensics reporting, and even in-depth mental health treatment features for adults and children. FEI also added features to support SAMHSA's increasing use of discretionary grants requiring GPRA submissions and has kept pace with advancements in industry standards relating to security, billing, and behavioral health practice. The result is a modular system that allows customers to collaborate on reporting, new features, and the management of specific programs for better reporting and outcomes.

By implementing WITS, the West Virginia Department of Health and Human Resources, Bureau for Behavioral Health (WVDHHR) obtains a partner who has extensive and specific knowledge of the design, validations, edits, and technical requirements needed for consistent and successful data sharing and integration between state data systems and SAMHSA, as well as a rich understanding of state and county needs in relation to behavioral health prevention and treatment systems.

- *Software must have the capability to collect all SAMHSA required GPRA data and submit data to SPARS nightly. Information can be found at: <https://www.samhsa.gov/grants/gpra-measurement-tools> and <https://spars.samhsa.gov/> [CRFQ 4.1.2]*

As shown in **Exhibit 2**—a snapshot of the follow-up dashboard using data from a test system—the GPRA management feature of the system is designed to enforce the rules of each grant. It allows multiple grants to be managed in the same system. For instance, two customers currently manage the SOR, COVID, and Screening, Brief Intervention, and Referral to Treatment (SBIRT) grants simultaneously. These customers have set up their provider agencies so that each provider has access to the appropriate grants. This allows authorized users to quickly navigate to the GPRA screen and ensures that entry of the intake GPRA is tied to the specific grant-related program. The system provides an automated nightly feed of all completed GPRAs (including deletes and changes) to SPARS. In addition, a follow-up dashboard allows providers, as well as the State, to receive alerts about follow-up due dates and to monitor the follow-up rates for each grant.

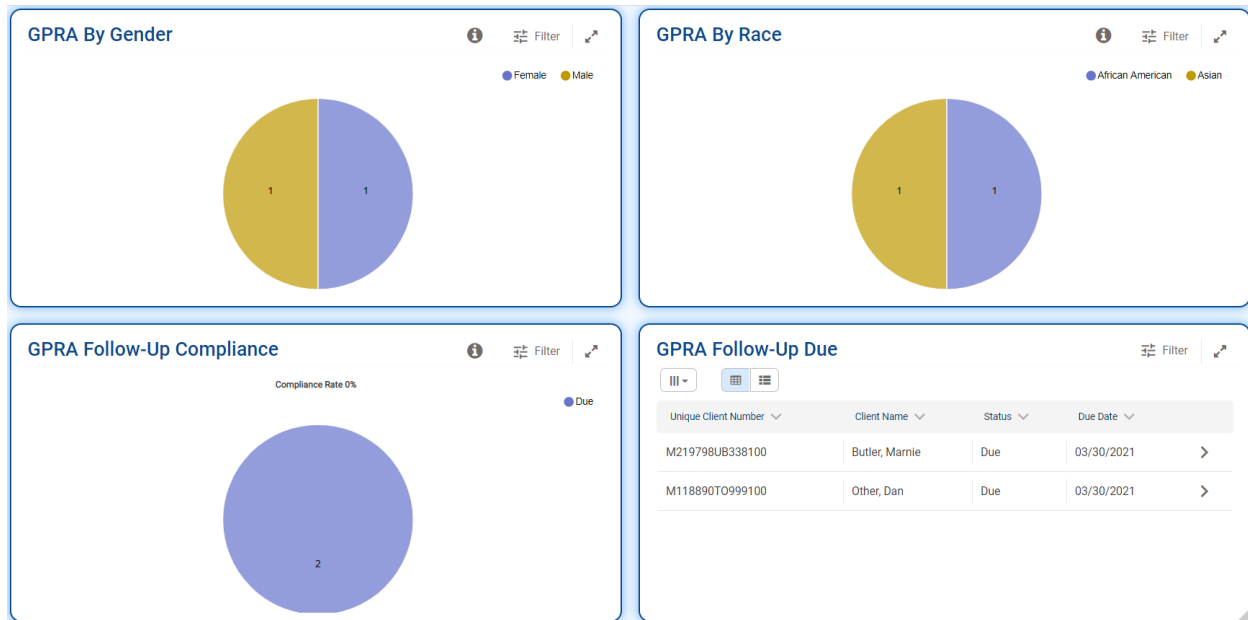


Exhibit 2. Grants Management Dashboard

Since FEI built SPARS (as a subcontractor to RTI), and the preceding SAIS and TRAC systems, FEI is uniquely positioned to ensure that all GPRA data entered in WITS is consistent with the upload protocols established by SPARS. The WITS GPRA module allows for entry of the GPRA and mimics all the rules in SPARS so that submissions are not rejected when they are uploaded each night. FEI has kept up to date with any new changes to the GPRA announced by SAMHSA (e.g., diagnosis, military history) and has rolled these out quickly to keep customers in compliance with their grant requirements.

FEI is currently supporting three SBIRT customers, 16 SOR customers, and seven COVID customers in the collection and automated upload of GPRA data to SPARS. West Virginia administrators will also be able to see the batch upload history, as well as any open error logs, from the WITS administrative screens. FEI's support staff monitor uploads as well on behalf of the State.

➔ *Software must include a 42 CFR Part 2 consent and referral process. Information can be found at: <https://www.samhsa.gov/about-us/who-we-are/laws-regulations/confidentiality-regulations-faqspe> [CRFQ 4.1.3]*

As part of the initial scope of work for SAMHSA's WITS project in 2002, FEI was charged with implementing a secure electronic consent and referral component of WITS that fully supported 42 CFR Part 2 regulations. This component has been reviewed and approved by the Legal Action Center in New York. This feature is useful in three ways:

1. In the administration of a discretionary grant, one entity may perform an intake GPRA. By using the consent/referral process to transfer the client to a new provider, the accepting provider can perform the follow-up assessment without needing to do a new intake GPRA. This preserves the integrity of data flow for grants and reduces work as well as confusion and allows the current treating provider to be able to perform the follow-up in a timely manner.
2. It also allows for transfer in treatment situations, so that there is better continuity of care if the client will continue treatment through a new Health Insurance Portability and Accountability Act (HIPAA) covered provider entity.
3. Finally, prevention specialists who may be working with an individual who has been identified as needing treatment may also refer that individual to a treatment agency, if desired.

The integrated consent and referral process allows a treatment or prevention provider to obtain the consent of a client to share specific elements of the treatment episode with another provider agency (another HIPAA-covered entity). Once signed by the client, the information is electronically visible by the other provider agency but is protected from re-disclosure.

Compliant with 42 CFR Part 2, the consent module in WITS records:

- The client who is consenting the information
- The disclosed from agency
- The disclosed to agency
- The purpose for disclosure
- The beginning date (earliest date of services to be consented)
- The domains of information to be consented and the expiration of each of those

In the example in **Exhibit 3**, each domain expires 180 days after the signing of the consent.

Client Disclosure Agreement

Hide Context Information

Note: Consented information may not be redisclosed.

Client Name	Unique Client Number	Disclosed From Agency
Violet, Sara	6453ZJ6875M5352	Test Training Agency

Entities with Disclosure Agreements

System Agency
☒ Yes ☐ No

Disclosed To Agency

Facility

Disclosed To Entity (Non System Agency)

Purpose for Disclosure

Earliest Date of Services to be Consented

Has the client signed the paper agreement form
☒ Yes ☐ No

Date Client Signed Consent

Client Information To Be Consented

**Expiration type is required for disclosure activities.*

Expiration Type

**Expiration type is required for Disclosure activities.*

Client Information Options

- Admission
- ASAM
- ATR Eligibility Screen
- Behavioral Health Assessment
- CAGE-AID Screening
- Consent
- CONTINUUM Triage™ Assessment
- CONTINUUM™
- DENS ASI Assessment
- DENS ASI Lite
- Diagnosis List

Disclosure Selection

- Client Information (Profile) (DS, +180)
- Client Screening (DS, +180)
- GPRA Interview (DS, +180)
- Intake Transaction (DS, +180)

Exhibit 3. Client Consent Form Page

The Client Disclosure Agreement box shows when the client has signed the consent, either electronically or on paper. Once signed, the consent becomes part of the clinical record and is read-only. The client's consent may be revoked by the client, at which point any further sharing of information is halted by the system.

The information consented by the client will be visible electronically to the disclosed agency (in this case, SOR Training Agency) through their client screen in WITS. Some WITS customers limit the sharing of information further by specifying either a sub-location within the receiving agency (called a facility in WITS) or by sharing only the data from one episode of care (regardless of the dates of client consent).

- ➡ *Software must allow and support access to approximately 550 users throughout West Virginia. Software must also include access and support for approximately 40 CO-Triage® users. Software must allow for the assignment of differing levels of system access to those users. External users will consist of clinical providers, treatment providers, WVDHHR staff, federal grant funded programs, and others as identified by BBH. Costs of any necessary licenses to support the software must be included in the bid. [CRFQ 4.1.4]*

The WITS system will support and provide access to West Virginia's approximately 550 users and 40 CO-Triage users. Currently, the largest WITS implementation has approximately 2,700 users, with no system degradation. In addition, WVDHHR can add new users without worrying about licensing costs, as FEI does not charge a per-user fee for the use of the WITS system. The only per-user licensing/subscription fees FEI charges are associated with copyrighted instruments, such as the ASAM CO-Triage and the ASAM CONTINUUM. FEI has included per-user subscription costs for the CO-Triage (40 users) and has also assumed per-user subscription costs for 525 CONTINUUM users based on the requested training from the Centralized Request for Quote (CRFQ).

WITS user roles and business rules allow WVDHHR to provide different levels of system access and functionality to those users as needed. WVDHHR or its providers (should they be given permission by the State) can easily modify users as well as their roles of access as staff change over time. WVDHHR is the only entity that can provide broad, multi-agency access to the system. Each provider agency will only view its own data and have access to its own staff.

The WITS system uses role-based authorization to control access to data, actions, and modules. Roles consist of a collection of permissions that give access to a set of screens and/or functions. In addition, Administrators can add, remove, edit, and reset credentials as needed.

WITS has roles for state-level users (who may have access across all agencies in the State), as well as roles for County Authorities or Sub-Recipients, who only have access to their own entity in the system. Additionally, there are roles to allow access to features such as prevention implementation, client data entry, or reporting. Upon creation of the user's staff account, the system will generate an email to the user to allow them to set their own credentials. Users can generate their own credential reset, or this can be done by a staff administrator.

- ➡ *Software must create ad-hoc reports as identified in 3.1 Mandatory Contract Services Requirements, Deliverables, and Timeline. Reports should be able to be run by both internal and external users based upon the level of access to the system. Other reports will be added as needed. [CRFQ 4.1.5]*

Any user granted permission by the state, whether internal or external, can run or build ad hoc or other reports from WITS via access to Microsoft's SSRS. FEI allows the reports to be generated against a real-time copy of the production database, so information is always up to date and long running reports do not degrade performance for those using the system. The SSRS reporting environment is SSO from WITS and uses the assigned permissions of the user to determine which data is available to them for reporting. For instance, any provider will only be able to report on data from their own organization. A provider (or

the state) may build a report that can be published to all providers and each provider will only be able to see his or her own data. On the other hand, the state may build reports that allow for access across all provider entities.

SSRS allows for the development of new ad-hoc reports or stored reports in table/matrix views graphical views and may include heat mapping data as well. In addition, “form letter” reports can be built and used to create mailings or other communications to individuals within the database.

Data is available in real time in the SSRS workspace. Saved reports can be “subscribed” and sent to people using secure email. The state will have control over the organization of the reports in SSRS and how they are stored, as well as the people who have access to run or build reports. FEI’s support team aids and provides trouble-shooting with report building as needed to the state.

Furthermore, WITS customers can generate both the SUD Treatment and Prevention block grant reports from the information that provider agencies enter the WITS live system. This is done through the SSRS reporting access mentioned above. The SSRS reports are set up so State staff can run the report for all agencies for a specified period or a single agency at a time. This feature allows state staff the opportunity to review the results with its providers before providing the annual reports to SAMHSA’s WebBGAS system. As each state has a slightly different way of reporting block grant data, FEI will work with West Virginia to align these reports with the data collected in WITS. **Exhibit 4** represents a sample Substance Abuse Block Grant report.

SABG Primary Prevention Expenditures by Institute of Medicine (IOM) Categories					
SABG Table 5b					
Report Period- From: 10/1/2018 To: 9/30/2019					
Report Run Date: 12/14/2019					
Regional Prevention Provider					
Activity	SA Block Grant Award	Other Federal	State Funds	Local Funds	Other
Universal Direct	\$24,000	\$0	\$8,000	\$0	\$2,300
Universal Indirect	\$18,000	\$4,700	\$12,000	\$400	\$0
Selective	\$0	\$0	\$0	\$0	\$0
Indicated	\$0	\$0	\$0	\$0	\$0
Column Total	\$42,000	\$4,700	\$20,000	\$400	\$2,300
Total SABG Award	\$50,000	\$5,000			
Planned Primary Prevention Percentage	84%	94%			

Exhibit 4. Sample Prevention Block Grant Report from SSRS

If the state wishes, tools such as Power BI, Tableau, or other commercial products can be layered on top of the SSRS data structures maintained by FEI. Several current WITS customers use these tools for further data reporting.

2.2 Standards of Privacy and Security [CRFQ 4.2]

Software must provide support for HIPAA compliance. [CRFQ 4.2.1]

Because of the scope of services we provide, the type of companies and partners with whom we work, and the nature of the markets we serve, FEI finds itself directly or indirectly subject to a comprehensive set of requirements that likely exceed those with which any individual customer must comply. This comprehensive body of legal and regulatory mandates includes, but is not necessarily limited to those listed below:

- | | |
|--------------------------------|-----------------------------|
| ▪ BPSSM | ▪ HIPAA/ARRA/HITECH/PPACA |
| ▪ CA1386 / MA 201 / State Laws | ▪ IRS Regulations |
| ▪ CoBIT / ITIL / ISO27000 | ▪ NISPOM / DITSCAP / DIACAP |
| ▪ Computer Security Act | ▪ NIST SP 800 Series |
| ▪ Customer Requirements | ▪ OIG/CFO/EDP |
| ▪ FISMA/FISCAM | ▪ OMB A-123, A-130 |
| ▪ FTC Section 5 | ▪ Privacy Act |
| ▪ HHS SecureOne | ▪ PDDs / HSPDs |

FEI believes that it is important to meet all of the requirements of the above mandates. However, rather than chase each mandate individually, FEI has adopted a strategic approach by establishing an enterprise-wide Privacy, Risk, & Information Security Management (PRISM) function and stipulating that consideration of these issues be integral to our business activities, organization culture, and interpersonal environment.

Strategy

Three core themes serve as the basis for FEI's PRISM Program. First, make security a top management priority. Second, create a program to encompass the full spectrum of requirements. Third, satisfy these requirements in the most efficient way possible.

Every member of FEI, no matter what their status (employee, contractor, consultant, temporary, senior vice president, or other), is subject to the same information security requirements, has the same relative responsibilities to support FEI security objectives, and must comply with FEI's enterprise security rules and procedures.

Beyond making security everyone's responsibility in general, others within FEI have specific security responsibilities. For example, the members of FEI's Executive Leadership Team are well aware that their collective role is to oversee the company's organizational strategies, structures, systems, staff, and standards. However, in setting the "Tone-From-the-Top," FEI management does not limit itself to a traditional definition of the scope of their purview. Instead, FEI fully recognizes our reliance on information technology (IT) for competitive advantage and has established an enterprise culture of due diligence.

In less abstract terms, this means that FEI's Executive Leadership Team takes an active role in the governance of the organization and maintains ongoing awareness of our risk exposure. FEI has established a program to comply with critical elements across the full spectrum of governance. Integral to this effort is the management level representatives who have been assigned responsibility for IT, IT Governance, IT Security, Information Security, and ultimately, Information Security Governance.

All told, FEI Executive Management Team fulfills its compliance obligation by extending its governance reach to provide the leadership, organizational structures, and processes that ensure everyone throughout the enterprise supports and sustains our strategies and objectives.

As the final element of our strategic approach, FEI has developed a master control framework in which we have adopted a standard set of control objectives (and underlying control techniques) that have been designed to satisfy ALL of the various requirements of the individual mandates to which we are subject. To substantiate the level of rigor our Executive Leadership Team requires, to enable distributed support throughout the organization, and to provide internal and external parties with the level of assurance needed, this control framework offers traceability between the requirements of individual mandates and the core mechanisms FEI has implemented in satisfaction thereof.

Compliance Hierarchy and Controls Inheritance

FEI's management team has prudently adopted a strategic approach by establishing an enterprise-wide Information Assurance Program and by stipulating that risk management be integral to our business activities, organization culture, and interpersonal environment. Beyond the broad policy setting direction described above, FEI has also taken tactical steps to satisfy the full spectrum of requirements to which each of our programs is respectively subjected. Specifically, as depicted in **Exhibit 5**, we have adopted a hierarchical inheritance approach to controls fulfillment.

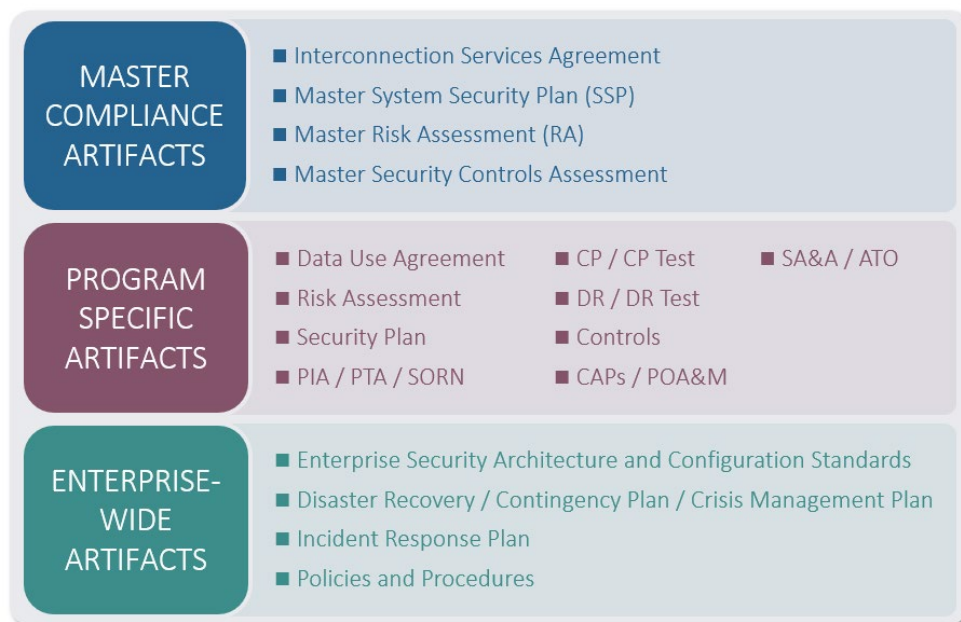


Exhibit 5. Controls Hierarchy and Inheritance Structure

FEI's Controls Framework is comprised of three tiers as described below:

- **Master Compliance Artifacts** – As the top tier of our program, FEI has established and maintains a library of master artifacts that apply to our organization. These items focus on the control objectives that are the same and are therefore said to be inherited by each of our individual programs. For example, included within our Human Resources program are various processes and procedures that satisfy the personnel security controls to which we are subject. This would include things like annotating personnel security level designations on position descriptions, conducting background investigations for all personnel, establishing an acceptable use policy, and formalizing disciplinary guidelines for violations of security policy. Because these activities are the same for every program,

they are documented in a single master artifact. This has the added benefit of reducing the overhead burden to maintain such documents and promoting greater document consistency and currency.

- **Program Specific Artifacts** – The middle tier of our control framework addresses the requirements that are unique to each program, system, customer, or contract. This consists of the agency/customer specific set of artifacts required for a certification package pursuant to the system’s Authority to Operate. It is at this layer where the variable aspects of systems/programs are captured. For example, the criticality of a system, the nature of the information processed within, the diversity of the user population (e.g., organizational vs. non-organizational users), the location and architecture of the system, all affect the systems’ risk exposure and drive the corresponding controls that must be adopted. These questions then would all be items answered by the artifacts maintained at this level.
- **Enterprise-Wide Standards** – Consistent with our philosophy that security is no different from any other quality measure, that showing respect for individual privacy concerns is key to customer satisfaction, and that long-term consistent value delivery can best be realized through a system of governance, we have established a foundation that provides the underpinnings of our entire program. Specifically, based largely on doing what we already know we need to do, and informed by models such as CoBIT, Information Technology Infrastructure Library (ITIL), International Organization for Standardization (ISO)27k, National Institute of Standards and Technology (NIST) SP 800-53, Health Information Trust Alliance (HITRUST) Common Security Framework (CSF), and others, we have implemented a set of policies, procedures, standards, and practices that assures operations are conducted most effectively without exposing our customers or us to undue levels of risk. This means that we satisfy most compliance mandates by default and are otherwise well positioned for ever-increasing demands for additional rigor. Finally, included within this tier are two additional capabilities vital to the success of all of our operations. Because IT operations and data are central to everything we do, we have centralized the establishment, routine testing, and ongoing refinement of both Incident Response and Disaster Recovery/Contingency Planning (DR/CP) Programs.

The elegance of the foregoing approach can be seen best by example. In a situation in which one of the many programs we conduct is subject to a security assessment or audit (e.g., 1/3 SCA, Annual Federal Information Security Management Act (FISMA) Assessment, HITRUST CSF, SSAE16, etc.), the independent evaluation team would rightfully expect to see a full set of artifacts to describe how control objectives are met across the full breadth and depth of the accreditation boundary. Thus, for any given program we would furnish the assessors with copies of the artifacts specific to that system along with copies of our enterprise standards and master artifacts. Were another system to be examined, a different set of program specific artifacts would be provided, but the same enterprise standards and master artifacts would again be referenced.

HITRUST Certified

Both the application and associated hosting environment have undergone a third-party HITRUST audit and received certification from HITRUST (2021)

☞ *All data is property of the WVDHHR, BBH. [CRFQ 4.2.2]*

FEI agrees with this statement; all data is the property of the WVDHHR, Bureau for Behavioral Health (BBH).

☞ *Upon termination of the contract, the WVDHHR, BBH will own all data collected and stored within the web-based data collection system. This will include all historical data to ensure the State can meet all federal reporting requirements. The Vendor will turn all data over to WVDHHR, BBH. Vendor will work with*

identified staff to determine the format of the data transfer. Data transfer would be conducted within 90 days of contract termination. [CRFQ 4.2.3]

FEI agrees that WVDHHR, BBH own all data collected and stored within the web-based data collection system including all historical data. Upon the termination of the contract, FEI works with WVDHHR, BBH to determine the format of the data transfer. Generally, FEI prefers to send the backup file using the built in SQL Server database backup mechanism, which produces a .BAK file. This file can be restored in a local SQL Server instance to which the Department has access. If a .BAK file is not practical for the Department, FEI works with WVDHHR, BBH officials to provide the database backup in a suitable format. FEI agrees to complete the data transfer within 90 days of contract termination.

- ➡ *Vendor must sign a security safeguards policy and confidentiality agreement and ensure privacy of data prior to contract award. These can be found at: <https://privacy.wv.gov/privacypolicies/Pages/default.aspx> [CRFQ 4.2.4]*

FEI has reviewed both documents referenced (West Virginia Executive Branch Confidentiality Agreement and Security Safeguards Policy - WVEB-P106). FEI will sign both documents upon award. Additionally, FEI has confirmed that our current information security and privacy program meets or exceeds all requirements specified in the policy documents.

- ➡ *The vendor will maintain application security to prevent unauthorized access to or disclosure of data transmissions [CRFQ 4.2.5].*

FEI has developed and maintains a comprehensive security and privacy program. The program is HITRUST certified. Below is a brief description of the major domains and associated control implementations.

Physical and Environmental (FEI Facilities)

Like most organizations with a suitable culture of security, FEI subscribes to the “defense-in-depth” approach to security. By this we mean that we employ various methods in a comprehensive layering tactic to ensure that if a given attack can penetrate one layer, other defense mechanisms will remain that not only help us prevent security breaches, but also provide us time to detect and respond to an attack, thereby reducing and mitigating the consequences of a breach. Thus, concerning the many IT support operations we conduct on behalf of healthcare customers, our outermost defense layer consists of the physical security controls described below:

- **Facility Security** – FEI conducts operations in support of its customers from one or more of its several facilities all of which meet or exceed FISMA and HIPAA physical security and environmental control requirements. Specifically, all of our facilities have been designed with designated entry/exit points governed with access controls as described below. All portals are also alarmed with audible alerts and/or sirens and logical transmissions fed to an alarm monitoring station. Locally we also have prop alarms on critical doors to ensure that they are properly closed. Wherever possible we have officially designated areas as publicly accessible and have segregated these spaces from those in which restricted information is handled and/or processed. Finally, one or more multiple barrier combinations are used (e.g., locked outer perimeter/secured interior perimeter/locked container) to further restrict access to Protected Health Information (PHI)/ Personally Identifiable Information (PII) and other sensitive information entrusted to us for safekeeping.
- **Card Access** – Sensitive information is contained in areas with key card entry where the Card Key Security System uses magnetic locks or electric strikes for security. It is installed at all strategic points of entry and the system is capable of producing reports for each entry point to show who has access, when it occurred, and who has been denied access.
- **Key Control** – Primarily as a backup mechanism to card access systems for use in power outages, a limited number of physical keys have been issued for perimeter portals and internal doors.

Assignment of these keys is strictly controlled and is managed by our facilities personnel. Additionally, along with changing codes to cyberlocks, physical locks for sensitive locations are rekeyed when keys are lost, combinations are compromised, or the affected individuals are transferred or terminated.

- **Telecom Closets** – Access to telephone closets and information system distribution and transmission lines within organizational facilities is limited only to authorized personnel. These controls extend not only to our personnel but to those of the engineering and building management teams of the facilities we occupy. Additionally, all physical ports are disabled by default until their use is needed. Like our data center and other secure facilities, telecom closet access is governed by badge readers under our internal control and access to these rooms is audited at a more frequent interval.
- **Alarm System** – Our facilities are all covered with intrusion alarms with portal sensors and motion detectors. The system does not rely on shared arm/disarm codes but rather requires a valid card key to activate or deactivate the system. The alarm sounds locally, and a signal is sent (with site location and event code information) to a monitoring service, which provides round-the-clock coverage. In turn, our alarm service contacts our security team based on predefined call procedures and escalation codes. Police are dispatched as appropriate.
- **Cameras** – Motion sensitive cameras are in place throughout the Data Center facility, providing video recorded egress, ingress, and internal activity. These cameras are motion sensitive and record all activity to a DVR for online retention. Permanent records are made each month to physical media for long-term retention. The DVR is also monitored for uptime and has alerts that warn when defined disk capacity thresholds are reached to ensure that records can be archived as necessary should volume exceed normal.
- **Visitor Management** – A formally defined visitor management program exists. Reception staff checks all personnel coming into and out of our facilities. Personnel who do not possess a badge for the facility must sign in. All visitors must present a US Government-issued picture ID and are presented with a visitor badge that must be worn visibly throughout the entirety of their stay. Guests must be signed in by a sponsor, an employee who will be responsible for escorting them at all times. Visitors and their belongings are subject to search and must note the serial number of any IT assets they bring into the facility to ensure that there is no confusion as to the ownership of said assets upon departure. Complete visitor access records are kept with detailed information and the logs are actively reviewed and verified monthly.
- **Environmental Controls** – Fire detection and protection systems provide continuous smoke and fire monitoring of the facility. A dedicated pre-action sprinkler system coupled with quick on/off sprinkler heads assures necessary fire suppression capability while minimizing the threat of accidental water deployment.

Asset Management

FEI uses Microsoft System Center Configuration Manager (SCCM) for asset management, which provides comprehensive and flexible asset management computer inventory asset management processes from deployment to retirement, including asset data audit, tracking, compliance, and reconciliation. It tracks non-computer and computer assets in a single configuration management database, teleconferencing gear, and other high value assets. Computer inventory and asset data are audited automatically on an ongoing basis. In addition, once asset data is rationalized, our asset management system enables asset tracking through the lifecycle including move, add, change, and delete activities.

Configuration Management

FEI uses manufacturer recommended hardware and software-hardening settings to minimize the system risk exposure. Additionally, FEI adopts and configures assets upon which customer hosted operations depend in accordance with industry standard baselines as promulgated by organizations such as the US

Government Configuration Baseline and the National Checklist Program. To the degree that it becomes necessary, we will also identify, document, and seek approval from customers for any deviations from established configuration settings for individual components necessary to fulfill explicit operational requirements. Lastly, using tools like SCCM and Tenable, FEI monitors and controls changes to configuration settings in accordance with organizational policies and procedures.

Vulnerability Management

FEI uses Nessus scanners in conjunction with the Tenable Security Center (TSC) to manage vulnerability scans of its network. TSC has been configured to scan each FEI subnet on a weekly basis. Configurations with the system and our routing and security rules allow TSC to check each IP in each zone to see if it is being used, and if so, to run a series of scans against each IP to identify the asset type, and check for known vulnerabilities. TSC performs both fully authenticated scans and unauthenticated scans to ensure comprehensive coverage. Results are stored in TSC for review and historical recordkeeping, and various reports created from this data are issued by TSC to various personnel in FEI to prioritize corrective action. Depending on the report, the creation could be monthly (trending) weekly (corrective prioritization), or multiple times a week (key items to focus on) to ensure that the team has a complete picture of the vulnerability posture of the network. Additionally, TSC is set up to issue immediate email alerts to specific staff if certain issues are discovered during a scan (FTP in use, generic password, etc.) so that these issues can be corrected immediately.

The timeframe for remediating vulnerabilities varies depending on the risk value of the vulnerability. Risk value is based on the severity of the vulnerability itself, potential for exploit, and impact. Standard patching is performed on a monthly basis, following the Microsoft patch Tuesday release. Patches are staged into a test/development environment before release to production. If a vulnerability is determined to be of high risk, patches or compensating controls will be implemented off cycle. This off-cycle deployment will also follow change control procedures.

Code Vulnerability Management

FEI uses Fortify on Demand (FoD) software to perform Static Application Security Tests (SAST) on developed applications. FoD has been configured to scan Development branches on a weekly basis and an integration within our Integrated Development Environment (IDE) may run a SAST on demand. The results of the scans are stored within FoD and a summary report is automatically generated and sent via email to the project data architect, development teams, and other pertinent stakeholders. The data architect and development teams review the report and complete an issue audit. During the issue audit, each vulnerability is reviewed, and depending on the level of risk further actions are identified. Risk is evaluated in accordance to Criticality, Likelihood, Impact, and existence of compensating controls. False positives are marked as such and a detailed description and evidence of why a vulnerability is a false positive accompanies these items, which are then submitted to Fortify for review. Fortify responds with a decision, which is reviewed by the FEI security team for final disposition. If the FEI security team unanimously agrees the vulnerability is a false positive, the issue will be suppressed in future scans.

Data Protection

All services provided by FEI are conducted in accordance with our defined Encryption Standard, which stipulates when such data protection measures are required and what methods are to be used accordingly:

- **Either Data in Motion** – For information in transit, data is encrypted directly or transmission is restricted to protected tunnels.

- **Data at Rest (Endpoints)** – Our personnel is formally trained for security, privacy, and the associated handling of sensitive data. Team members take corresponding precautions to protect data and do not store sensitive information on their desktops, workstations, laptops, or mobile devices. Nevertheless, for 100 percent of FEI portable endpoints (i.e., laptops and notebooks), we apply whole disk encryption to protect information at rest.
- **Data at Rest (Servers/SAN)** – Similar to any end point, FEI encrypts data at rest on our server infrastructure. In all cases, FEI leverages encryption algorithms that are Federal Information Processing Standard (FIPS) 140-2 validated. In the case of cloud deployed solutions, volumes are encrypted with FEI managed keys.

Continuous Monitoring (Threat and Activity Management)

FEI assumes responsibility for monitoring emerging information security threats and vulnerabilities and the necessary remediation. Our process for continuous monitoring/threat and activity management is described below. In satisfaction of applicable threat and activity management requirements, FEI applies audit, logging, and threat intelligence controls both to its own environment as well the entirety of the system's authorization boundaries (whether at FEI or within the public cloud) in which customer-facing systems are deployed. We have an enterprise security architecture based on the point product solutions with capabilities prescribed by NIST/FISMA to ensure coverage across our enterprise for the spectrum of threats to which we are subject. For example, to meet activity management control objectives, we use a 24/7 Security Operations center that leverages industry best practices tools (e.g., FireEye Helix) to provide a continuous view of the environment. This combination ensures that all security alerts and events are immediately reviewed and triaged by security professionals.

Events and alerts from cloud services (AWS CloudTrail/CloudWatch, Azure Monitor/Log Analytics), firewalls, SSL VPN Appliances, IDP Series ID/IDP Appliances, Windows security events, netflows, and other devices/capabilities are directed to a single location where they can be viewed and queried. In addition, events from different devices that indicate similar or identical security threats are normalized and categorized to enable easier analysis. Hereto, verbose logs from application components, servers, and network devices are captured and fed to correlation engines which detect the state of our devices for threat indicators, evaluate events to determine severity, accuracy, and context, and they then quickly escalate critical events to the attention of our Security Operations Center for further action to thwart compromise and/or other timely resolution.

Policies and Procedures

Every member of FEI, no matter their status (i.e., employee, contractor, consultant, temporary, senior vice president), is subject to the same information security requirements, has the same relative responsibilities to support FEI security objectives, and must comply with FEI enterprise security rules and procedures.

FEI established a process according to which information security policy is developed and maintained. In adherence with this process, PRISM continually monitors both the internal and external environments to identify required and desirable enhancements to its policy and program. Although such enhancements may be introduced at any time—for example, to comply with a new regulatory mandate—FEI formally updates and certifies its program no less than once per year.

Our objective in establishing an information security policy is the creation and maintenance of a “culture of security” in which FEI personnel throughout the enterprise naturally engage in appropriate security-oriented behavior. Similarly, our people represent one of our most effective weapons in information security, especially when equipped to identify and thwart improper behavior. However, this objective can never be accomplished if we fail to make workers fully aware of the nature of our pursuits. Therefore, FEI

established and maintains an internal information portal, with specific content dedicated to security, the purpose of which is to:

- Acquaint workers with information security risks and the expected ways to address threats faced
- Clarify worker responsibilities and duties for the protection of information resources
- Enable managers and other workers to make appropriate decisions about information security
- Coordinate efforts of different groups to protect information properly, consistently, and efficiently
- Provide guidance for the performance of information system security audits and risk assessments

All must comply with this policy and are required to sign formal annual acknowledgments to this effect.

Information Handling

FEI recognizes that its own information, as well as information that has been entrusted to us for safekeeping, must be protected in a manner commensurate with its sensitivity and criticality. Furthermore, we require that security measures be employed regardless of the media on which information is stored (paper, overhead transparency, computer bits, etc.), the systems that process it (PCs, firewalls, voice mail systems, etc.), and the methods by which it is moved (e-mail, face-to-face conversation, etc.). FEI also requires that information be consistently protected no matter what its stage in the life cycle from origination to destruction.

FEI has formally adopted an information classification system that categorizes information accordingly to four groupings. Specifically, all information under FEI's control, whether generated internally or externally, shall be deemed to fall into one of the following categories:

- **Public** – Information officially approved for release by FEI for widespread public disclosure. Generally, this information may be shared with anyone via any method because it is designed for public consumption and there is little to no inherent risk. Examples of information in the public category would be our marketing collateral or information on our public facing website.
- **Internal Use Only** – Information that is generally limited to FEI personnel only and is not to be disclosed outside the company. NOTE: In this context, the audience with whom Internal Use Only information may be shared is anyone to whom we have afforded physical and/or logical access to our facilities and/or systems regardless of the nature of their employment relationship with the company.
- **Confidential** – Information that would be considered sensitive internal information, disclosure of which would have severe public perception and/or financial repercussions. Access to information of this nature is restricted specifically to associates having a business "Need-to-Know." In plain terms, what this means is that the mere fact that someone is part of the organization and otherwise authorized access to Internal Use Only information does not by itself justify access to confidential information.
- **Restricted** – Information that is highly sensitive and because of legal or regulatory requirements typically requires special protective measures including multiple physical and logical security controls. Data types like PHI under HIPAA, PII under the Privacy Act, or Federal Tax Information under IRS 1075 would all fall into this category.

All associates are expected to familiarize themselves with the above definitions and the steps that must be taken to properly categorize the information assets for which they are responsible. To help Information Owners fulfill this responsibility, FEI has developed an internal online information classification applet that can be used in determining an asset's sensitivity.

Beyond categorizing assets into the appropriate category, associates must then ensure that the corresponding procedures are followed for handling information of different sensitivity levels in various use cases. To promote widespread adherence to this policy, FEI designed an Information Handling Matrix

to summarize our policies concerning the required, allowable, and prohibited activities associated with each classification.

NOTE: Based on the foregoing classification scheme, data, information/documents received from or created on behalf of Covered Entities would by definition be considered sensitive (e.g., either confidential or restricted), and as such care would be taken to ensure their security and privacy. Said assets would be stored securely in access-restricted shares subject to all applicable FISMA and HIPAA controls needed to govern access.

Personnel Security

All personnel performing services on behalf of a covered entity or other similarly regulated customers, who require access to our systems, facilities, or sensitive PHI/PII data, are subject to background investigations. Specifically, the FEI team works with our customers to perform position sensitivity analyses for all personnel to determine the applicability of this requirement and the corresponding level of background investigation indicated. Additionally, supporting the FEI Program Team is an embedded member of our security department who serves as a Security Investigative Liaison to facilitate this process acting as the single point of contact for such investigations. This ensures that customers receive timely written notification of all terminations/resignations of team personnel.

Whether or not a formal external background investigation is required, FEI subjects all of its personnel to a background examination (and periodic reinvestigation) process. Minimally, references and previous employment experience are verified for all employees. Beyond this, either a detailed or an exhaustive background check is performed based on the position's nature and need-to-know. Possible components include examination of criminal conviction records, lawsuit records, credit bureau records, driver's license records, as well as verification of previous employment. This control applies to new employees, re-hired employees, transferred employees, as well as third parties, such as temporaries, contractors, and consultants.

Security Training and Awareness

All FEI associates are trained on our security policies and procedures, as well as relevant aspects of the HIPAA Security and Privacy Rules, the Privacy Act, and the Freedom of Information Act. Specifically, on their first day of work, every individual is provided with a security orientation to make them aware of their responsibilities under our security program and to call their attention to the elements of greatest importance such as handling procedures for sensitive information. Additionally, on an annual basis, Security Training and Awareness is provided for all associates (including interns, temporary staff, and contractors). Complementing our training program, regularly, all personnel receive security program awareness bulletins directly in their inboxes on relevant topics of interest. Along with posters, periodic contests, and campaigns, these activities help ensure that security remains top of mind with all associates.

Beyond security awareness training, personnel with significant information security responsibilities (i.e., as part of their job) also receive additional functional security specific training (e.g., firewall administration, vulnerability management) on an annual basis. Professional certification is supported for all members of FEI's security and IT departments and most personnel have several. Finally, to the degree that customers wish to have FEI associates participate in their own security awareness training, we work closely to coordinate successful completion as needed.

Risk Management

In general, the purpose of a risk assessment is the recognition of the risks to which an organization is exposed. FEI seeks such an understanding because it is inconsistent with management due diligence to

accept risks simply because of lack of awareness. On the other hand, it is entirely in keeping with management's duty to accept a risk about which one is both cognizant and convinced that exposure is within tolerable limits. Thus, FEI's Executive Leadership Team, as well as the owners of each of our various LOBs, take active steps to learn what security problems (if any) exist and to have plans in place to resolve them.

FEI has developed a standardized Risk Management Process that is entirely consistent with both HIPAA and NIST guidance for use throughout the enterprise along with several assessment tools that are used to evaluate information security posture and degree of compliance with the policy. Based on this methodology, and as depicted in the FEI Master Control Framework presented above, two such risk assessments are conducted; one to capture system/program specific risks and another for FEI as an enterprise.

For the FEI enterprise risk assessment, on an annual basis, we conduct a formal Risk Assessment process, first internally and then with the assistance of an outside audit firm with an extensive background not only in leading information security and privacy practices, but also in FISMA, HIPAA, ISO, and ISO controls in particular. In the same manner that corrective action plans are developed and implemented for discrete risks associated with individual systems/programs, we create and track actions to remediate these enterprise risks accordingly.

- *Vendor must provide agency with a Security, Privacy, and Confidentiality Plan within 30 calendar days of contract award. [CRFQ 4.2.6]*

FEI will provide the agency with a West Virginia system specific Security, Privacy, and Confidentiality Plan within 30 calendar days of contract award.

- *The vendor will provide privacy protections equivalent to those provided by Standards for Privacy of Individually Identifiable Health Information, 45CFR Part 160 and Sub-Parts A & E of Part 164. <https://www.hhs.gov/sites/default/files/indroduction.pdf> [CRFQ 4.2.7]*

The FEI solution provides privacy protections equivalent to those provided by Standards for Privacy of Individually Identifiable Health Information, 45CFR Part 160 and Sub-Parts A & E of Part 164. The FEI system is designed in accordance with the minimum necessary, least privilege, and zero trust principles. Additionally, HIPAA compliant auditing is built into the core system, with complete separation from the transactional system. These design principles along with a comprehensive HITRUST certified application, hosting infrastructure, and hosting operations ensure full compliance with the stated regulations.

- *The vendor will notify the WVDHHR, BBH immediately by phone and email, provided upon award of contract, of any unlawful or unauthorized use or disclosure of PHI of which they become aware, if the data is determined to have been compromised. The vendor will provide all necessary details including, but not limited to, what data was compromised, when, how and by whom; and when they first became aware; and, they will provide a corrective action plan as to how any unlawful or unauthorized access will be avoided in the future. [CRFQ 4.2.8]*

For reportable occurrences, at the initial stage of the investigation, FEI makes no distinction between an event and an incident. In other words, everyone is instructed to err on the side of safety and report ALL possible violations of security/privacy. More specifically, users have been specifically instructed as to possible triggers, what to report, who to call, and how to report (including what information to provide).

The second part of FEI's Incident Response capability concerns how our Incident Response Team (IRT) responds to the reports we receive. The specific protocol and process for receiving, evaluating, responding to, reporting on, and managing all security and privacy events are defined in our plan. Also defined are the members of the IRT, an overlapping Incident Response Support Team, an Incident

Response Management Team, and the responsibilities of all teams and their individual members. Furthermore, different levels of response urgency and rigor are indicated based on whether an occurrence is classified as an event (i.e., of lesser concern) or an incident (i.e., of greater concern). Also defined, are the mechanisms for preserving the digital chain of custody for evidence that might be used in the event of prosecution as well as the formal command chain according to which information selectively flows upward to inform and support management decisions.

Finally, for incident reporting, FEI has a formally defined chain of command for internal approvals and a process for external reporting of security and privacy events according to which the affected customers would be notified of any incidents affecting their data or operations conducted on their behalf. As required, the incident report will contain all details associated with the event and investigation, which includes what data was compromised, when, how and by whom; and when/how the organization became aware of the incident.

- *The vendor will work with the WVDHHR, BBH and investigate and comply with any state or federal laws <http://www.technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2017PO1001SecuritySept2016.pdf> if any unlawful or unauthorized use for disclosure occurs including, but not limited to, payment of amounts deemed reasonable and necessary to mitigate the effects of breach. [CRFQ 4.2.9]*

FEI recognizes that every security incident is unique. As such, they require independent investigation and collaboration with our customers. For any reportable incident for the State's instance, FEI will work with the State or assigned contacts to ensure that a comprehensive investigation has been completed and that said investigation, findings and actions comply with applicable State and Federal laws.

- *The vendor will document and keep current its security measures as required by applicable law <http://www.technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2017PO1001SecuritySept2016.pdf>. [CRFQ 4.2.10]*

The FEI security program and policies are documented and kept current as required by applicable laws. Please refer to our response to HIPAA compliance for additional details on policy structure and inheritance. The FEI system and associated policies and procedures are both HITRUST and ISO 20000 certified. These standards certifications require annual third party audits to ensure ongoing compliance.

- *In the event of termination of vendor services, the vendor will surrender and transfer all data to WVDHHR, BBH, allowing for electronic download (file transfer protocol or FTP) within 90 days. After confirmation of successful transfer, the vendor will destroy all data to ensure data privacy. Please refer to 4.1.2.3. [CRFQ 4.2.11]*

Upon the termination of the contract, FEI will work with WVDHHR to complete the data transfer of all the data entered in the data collection system within 90 days of contract termination. FEI agrees to destroy all the data after confirmation of the successful transfer.

- *At the conclusion of the contract, or if the contract becomes void for any reason, all data (active directory users, databases and other pertinent licenses and software) will revert to the ownership of the WVDHHR, BBH. [CRFQ 4.2.12]*

FEI agrees that WVDHHR, BBH owns all data collected and stored within the web-based data collection system including all historical data. Upon the conclusion of the contract, FEI works with WVDHHR, BBH officials to provide the database backup in a suitable format. FEI agrees to complete the data transfer with 90 days of contract termination.

- *Contract item must meet or exceed the mandatory requirements listed below. Vendor should provide with their bid a copy of any hardware or software licensing and/or support terms and conditions which the State*

of West Virginia or the Agency must agree to or accept, either in writing or digitally, in order to order and receive the commodities or services offered as part of this contract. Written terms will be required prior to the award of any contract resulting from this solicitation. Failure to provide additional terms and conditions may result in disqualification of the vendor's bid. [CRFQ 4.2.13]

As described in **Section 2.3** of this response, FEI's WITS system meets or exceeds the mandatory requirements as set forth in this CRFQ. FEI has included responses to match the Deliverables as follows:

1. Implementation will support ASAM CONTINUUM and CO-Triage integration
2. State waitlist/bed management feature to support block grant priorities
3. Features to support the SOR Grant and GPRA uploads to SPARS
4. Prevention modules to support the SAPT block grant data collection
5. User Documentation
6. Training
7. Maintenance, Support, and Upgrades

FEI has provided a WITS Master Licensing Agreement, which is designed to indicate the terms of licensing of WITS to the State of West Virginia.

FEI's standard Service Level Agreements are provided in **Exhibit 6**.

Exhibit 6. WITS Issue Severity Matrix Ensures

Value	Level	Description
1	Critical	Critical defects are defined as system outages or anything that hampers the day-to-day operations of the WITS Platform for the majority of the end users, no workarounds have been defined and there is a potentially negative financial impact to the customer.
2	High	High defects are defined as any issue that frequently impacts some end users and a workaround has been identified
3	Medium	Medium defects are defined as an issue that infrequently impacts some end users
4	Low	Low defects are defined as something that rarely impacts a small number of end users

Once issues are assigned a severity, analysts investigate and follow up on issues adhering to the timeframes for each severity depicted in **Exhibit 7**.

Exhibit 7. Help Desk work items are addressed quickly based on WITS standard SLAs

Problem Level	Acknowledgement	Action Plan/First Follow-up	Status reporting and Resolution
Urgent(Critical)	2-3 hours	4-8 hours	12 hours
High	2-3 hours	8-12 hours	24 hours
Medium	4 hours	24 hours	40 hours
Low	4 hours	40 hours	80 hours

In addition, FEI has reviewed the Terms and Conditions set forth in the CRFQ and would like to offer the following modifications to these as part of the quoted price. The requested modifications appear in ***bold italics*** below.

1. **Section 8 – Insurance – Cyber Liability** – Currently reads as “\$10,000,000.” FEI's current customer base of over 40 states and counties all require \$5,000,000 or less. FEI would request a drop in this requirement to \$5,000,000.
2. **Section 27 – Assignment** – Add language at end to read as: “Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments, ***with such consent not being unreasonably withheld, delayed, or conditioned.***”

3. **Section 36 – Indemnification** – Please amend with highlighted text as follows: “The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against, *and to the extent:* (1) Any claims or losses for services rendered by any subcontract, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hours laws. *Additionally, each party (the “Indemnifying Party”) shall indemnify, defend, and hold harmless the other party, its affiliates, and their respective officers, directors, employees, representatives, agents, successors, and permitted assigns (the “Indemnified Party”) from and against any and all claims made or threatened by the other party or any third party and all related losses, expenses, damages, costs, and liabilities, including reasonable attorneys’ fees and expenses incurred in investigation or defense (“Damages”), to the extent such Damages arise out of or relate to: (i) any negligent or willful act or omission of the Indemnifying Party; or (ii) any breach in a material representation, covenant, or obligation of the Indemnifying Party contained in this Agreement.”*
4. **ADD SECTION 46 – “46. Limitation of Liability. NEITHER PARTY SHALL BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THIS AGREEMENT OR ARISING FROM OR RELATED TO A BREACH OF THIS AGREEMENT OR USE OF THE PRODUCTS AND VBA SERVICE, INCLUDING IN THEIR WHITE LABEL FORM, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF THESE DAMAGES. IN NO EVENT SHALL EITHER PARTY’S CUMULATIVE AND AGGREGATE LIABILITY ARISING OUT THIS AGREEMENT OR USE OF THE VBA SERVICE EXCEED THE GUARANTEED CONTRACT VALUE.”**

2.3 Deliverables, Scope of Work, and Timeframe [CRFQ 4.3]

2.3.1 Deliverable 1: ASAM CONTINUUM™ and CO-Triage® Integration [CRFQ 4.3.2]

- *The software application must utilize and integrate the ASAM CONTINUUM™ computerized structured interview and clinical decision support system (CDSS). [CRFQ 4.3.2.1]*

The WITS solution uses and integrates the ASAM CONTINUUM computerized structured interview and Clinical Decision Support System (CDSS). The CDSS includes the structured interview and the algorithm to determine the ASAM level of care. Because it is integrated with WITS, the data is synced within the WITS system so the level of care data can then be used within WITS for tracking and reporting.

- *The ASAM CONTINUUM™ comprehensive assessment will provide the treatment team with a means to conduct a biopsychosocial assessment of patient needs along the six ASAM Dimensions and determine a final recommended ASAM Level of Care placement, while facilitating utilization review. The decision engine must use research-quality questions (including tools such as the Addiction Severity Index or ASI; Clinical Institute Withdrawal Assessment for Alcohol or CIWA; and the Clinical Institute Narcotic Assessment or CINA) to generate a comprehensive patient report that includes the level of care placement. [CRFQ 4.3.2.2]*

The ASAM CONTINUUM comprehensive assessment provides the treatment team with the ability to conduct a biopsychosocial assessment of patient needs along the six ASAM Dimensions to determine the level of care. The integration with WITS automatically pulls back all assessment data as well as two structured reports from the ASAM system: a summary report as well as a detailed problem list that can be used to inform treatment planning.

The decision engine uses research-quality questions (including tools such as the Addiction Severity Index (ASI), Clinical Institute Withdrawal Assessment (CISA), and Clinical Institute Narcotic Assessment (CINA) instruments to generate a comprehensive patient report which includes a recommended level of care determination. Because FEI is an authorized ASAM CONTINUUM distributor, the tool comes directly from ASAM and is supported by ASAM.

- ➔ *Software application must utilize and integrate the short, 21-question ASAM CO-Triage® screener to deliver a preliminary ASAM Level of Care placement recommendation. [CRFQ 4.3.2.3]*

The WITS solution uses and integrates the ASAM CO-Triage screener to deliver a preliminary ASAM Level of Care placement recommendation. As with the ASAM CONTINUUM, it is integrated and syncs with the WITS solution seamlessly, making the data available for tracking and reporting. Because the ASAM CO-Triage data is saved, the user has the option to pull forward previously entered information for editing, thus reducing repeat data entry time for clinicians.

- ➔ *Timeline: Completion within twelve weeks of contract award. [CRFQ 4.3.2.4]*

FEI can make this integration with ASAM's Clinical Decision Support System, including access to both the ASAM CONTINUUM and ASAM CO-Triage, available in 12 weeks of contract award. Based on the number of training classes, FEI and ASAM have assumed that subscriptions will start on 9/30/2021.

2.3.2 Deliverable 2: Statewide Bed Waitlist and Management Module [CRFQ 4.3.3]

- ➔ *Provide a real-time, statewide/countywide bed availability and waitlist management module. Module must allow for the management of any program or modality of care across West Virginia, specifically the monitoring of inpatient hospital, psychiatric residential treatment facility, or other residential beds. Module must have the ability to provide compliance with requirements for priority access outlined in federal 45 C.F.R. § 96.131 Treatment Services for Pregnant Women and State §9-5-24, as well as availability of open spots for individuals not identified in federal regulations. [CRFQ 4.3.3.1]*

The WITS Platform contains capacity and waitlist tracking that will allow West Virginia to satisfy its need for a block-grant based Statewide Bed Waitlist and Management Module. Statewide waitlist management allows for the monitoring and management of any program or modality of care across the state, which means that the state and its providers can use the system to monitor bed-based program availability (residential, hospital, PRFT, etc.) and also slot-based availability (OP, IOP, special outreach programs) if desired. The sharing of information regarding available beds or slots and those waiting is done without breaking the confidentiality of the individuals waiting for beds.

Within WITS, the State will establish each of the various agencies that will use the system to manage bed or slot availability. Each agency represents a business entity that may have multiple locations or sites. Each location has its own identifying information that can be set up individually and is then associated back to the larger overall business entity. Each agency can be credentialled for various programs of service or levels of care; the setup of these specific programs includes capacity information that is used for the Statewide Waitlist and Management Module. Using the initial setup of agencies and their contracted programs, the State can include additional details such as capacity, as well as any gender, age, or other specifications for a program. Then the state, together with its providers, determines which programs will be monitored on the statewide waitlist. Each program may be set up to allow for inclusion on the statewide waitlist, be limited to the provider's clients, or have no waitlist.

Providers who have clients needing a residential bed, outpatient program, or other type of program, may search for programs by the level of care, location/region, number of available beds/slots, or gender/age specific programs (other search criteria can be added). The following screen shows a search for Short Term Residential beds. The screenshot below, taken from a test system, shows three short term

residential programs that are available on the waitlist. Their current available slots/beds (licensed beds minus filled beds), as well as the number of people waiting for beds for the program, are displayed. This view also shows any age or gender restrictions for the program.

Agency/Facility	Facility City	Program	Modality	Available Program Slots	# on Waitlist	Age/Gender	
County Assessment and Treatment Center/Greeley		Women's SUD Residential	Rehabilitation/Residential-Short Term (30 days or fewer)	9	6	None/Female	⋮
County Assessment and Treatment Center/Greeley		Residential SUD	Rehabilitation/Residential-Short Term (30 days or fewer)	6	0	None/None	⋮
Peer Drop In Center/Treatment		SUD Residential Short Term	Rehabilitation/Residential-Short Term (30 days or fewer)	14	4	None/None	⋮

Exhibit 8. Filtered List of Programs with Open Beds

Clicking on the ellipsis to the right reveals data regarding those waiting, without giving away any identifying information. This view is shown in the next exhibit, below. Note the time waiting, as well as a “score” are provided based on key data such as the person’s HIV, IV drug use, and pregnancy status. Any new client can be easily added to the waitlist by clicking the “Add” action in the upper left corner.

+ Add Client to Waitlist										
Waitlist ID	Placed by Agency	Gender	Age	Due Date	HIV Tested	IV Drug User	Days Waiting	Priority	Status	
21	County Assessment and Treatment Center	Female	15		No	Yes	208	2	Pending	⋮
35	County Assessment and Treatment Center	Female	21		No	No	12	0	Pending	⋮
28	SAC Kansas	Female	21	2/1/2021	Yes	No	191	5	Pending	⋮
34	SAC Kansas	Female	34	2/1/2021	Yes	Yes	127	6	Pending	⋮

Exhibit 9. List of Clients Waiting for a Program

Users with State Waitlist roles can manage and update the waitlist profiles for the clients their agency has placed on the waitlist. For instance, a female who was not pregnant at the time she was originally placed on the waitlist, can be updated if she becomes pregnant (which would increase her priority score). In addition, the Agencies that manage programs with waitlists may view and accept clients off the waitlist, all without sharing PHI. The integrated consent and referral process allows the data to be shared at the appropriate time for all the agencies that use the WITS platform.

Most powerfully, this feature allows the state to manage and monitor information such as bed availability for any program type or level of care, track client wait times, set priorities for certain types of clients (e.g., pregnant women, veterans), and pinpoint trends in bed availability by program type at the county, region or state level. All of this information is available in real-time. As a client is removed from the waitlist or enrolled in a program, the bed/slot availability automatically updates and is visible to all on the statewide waitlist.

➡ *Module must record and store authorization for care for residential services or other levels of care as part of the official client record. [CRFQ 4.3.3.2]*

Most customers using the ASAM CONTINUUM for an official level of care authorization will record the Recommended Level of Care coming directly from the CONTINUUM system as justification for the use of residential or other levels of care. When a CONTINUUM is completed, the user can pull back the full level of care recommendation into WITS. Most customers require the user to indicate the actual level of care, and if this differs from the CONTINUUM recommendation, they must supply a reason. This is displayed in

the image shown below, where the gray boxes represent information that has been pulled directly from CONTINUUM. The actual level of care, clinical override, and comment has been entered by the user.

Lowest Recommended Level of Care

4 - Medically Managed Intensive Inpatient

Clinical Override

Level of care not available

Recommended from CONTINUUM™

4 - Co-occurring Capable, 4-WM - Medically Managed Intensive Inpatient Withdrawal Management

Actual Level of Care

2.1 - Intensive Outpatient

Comments

There are no beds available in Morgantown for ASAM Level 4

Exhibit 10. ASAM CONTINUUM Level of Care Recommendation

Should the State wish to go a step further in recording a more official authorization which would include a specified number of services or length of stay, this can be easily stored as part of the client record. The user would simply enter the information (including an official authorization number) on the screen shown below. The image below shows a standard authorization for 30 days of residential care. In this case, the authorization is tied to a Medicaid payer.

0967112E 41 Male

Authorization

Hide Context Information

ID 5653

Administering Agency IDHRL DBH, Region 1

Created By Conrad, Jennifer A.

Created Date 4/7/2021 1:35 PM

Updated By Conrad, Jennifer A.

Updated Date 4/7/2021 1:35 PM

Group Enrollment Medicaid OP (3/1/2021-8/1/2021)

Status Active

Plan Medicaid (OP)

Authorization # 12345

Contract

Effective Date 3/1/2021

End Date 8/1/2021

Date Approved 3/7/2021

Comments

Authorized Services List

+ Add Service

Service	Authorized Units	Encumbered	Expended	Available Units
SR Residential	30	0.00	0.00	30.00

Total Authorized 30.00

Total Encumbered 0.00

Total Expended 0.00

Total Available 30.00

Exhibit 11. Client Service Authorization

April 13, 2021

Page 23

Should West Virginia choose to later add billing features to the system, the capture of authorizations and use of services can be automated within the system. This can be quoted later as an enhancement to the system should these more advanced features be desired.

- *Module must have the capability to allow BBH to track identified block grant data, and data regarding timely access to care as required by the Medicaid 1115 Waiver. [CRFQ 4.3.3.3]*

Within the scope of the current Statewide waitlist, it will be very easy to determine the timely access to care, and to evaluate that based on level of care as well as region and/or preference or risk category of the client. When a client is placed on a waitlist, it is directly related to a program, which has a defined modality/level of care and is also located at a specific address within the state. Information about the client is also gathered, as shown in the figure below, which includes the date placed on the waitlist, block grant priority information (such as pregnancy status – automatically set to null if the client is male, HIV or Chronic Life Threatening Illness (CLTI) status, IV Drug Use status), and additional priority information as determined by the state, for instance, State Probation/Parole as shown below. The priority scoring for the client below, based on scoring values set by the state, is “3.” This also helps the state issue guidance to providers regarding which clients should receive priority when beds/slots become available.

Client Readiness List Profile

Agency Central Valley Recovery Se	Facility Mothering Heights	Age/Gender None/None
Program Name Perinatal Residential	Modality Rehabilitation/Residential-Short Term (30 days or fewer)	
Available Slots 30	Readiness List Status Pending	Date on Readiness List 3/30/2021
Client Name Jones, Kyle	Unique Client Number KJ0030287	Gender Female
DOB 3/2/1987	Last 4 of SSN 2222	Pregnant Yes
Due Date 9/1/2021	IV Drug User No	CLTI No
Other Priority Options All Other Contract Pregnant/IV Users		Selected Priority Options State Probation/Parole
<div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="border: 2px solid red; padding: 5px;"> BG Priority 3 </div> <div> Add client to all readiness lists for this modality? <input type="radio"/> Yes <input checked="" type="radio"/> No </div> </div>		

Exhibit 12. Client Waitlist Profile captures required timeliness reporting data

When the client is accepted into a program, the date of acceptance is automatically recorded, and the client is removed from the waitlist. This information can be used along with the date they were placed on the waitlist, to fully determine the timeliness of their access to that specific program.

- ➡ *Module must be integrated within the larger, overall data reporting and case management software application. [CRFQ 4.3.3.4]*

The information shown in this section above is all part of the WITS platform and is in use by customers today.

- ➡ *Timeline: Completion within twelve weeks of contract award. [CRFQ 4.3.3.5]*

The waitlist feature is currently available in the WITS platform “out of the box” and the base features can be available within 12 weeks of contract award. FEI is assuming that users from each facility, who manage clients, will log into WITS and enroll a client in the program (to show a bed/slot being used) and disenroll a client (to show a bed/slot is now available). FEI will disable the TEDS requirements that normally accompany this process so that the enrollment and disenrollment processes are easily managed by users. These requirements can be enabled at a later date, under a different scope of work and pricing, should that be desired by the State.

2.3.3 Deliverable 3: State Opioid Response (SOR) Grant GPRA Reporting Module [CRFQ 4.3.4]

- ➡ *Module must allow for the entry of basic client data (utilizing the same profile as ASAM CONTINUUM™ and CO-Triage®) and entry of a client’s intake and enrollment into the SOR program of care, including the collection of **evidence-based service type and level of care**. **The use of evidence-based screeners and assessments for this module should include the Addiction Severity Index (ASI), ASI Lite, and ASAM criteria.** [CRFQ 4.3.4.1]*

The WITS Platform allows for the full capture of basic client data in the client profile. Once a client has been entered, the treatment agency does not need to enter this information again.

Once the Client Profile is completed and saved, the treatment agency can enter data regarding any program of care. This would include adding a GPRA and DENS-ASI or ASI Lite for SOR, as well as entering the CONTINUUM assessment, should that be required. Once the state’s required tools have been used to determine the level of care that is appropriate for treatment, the client can be associated with the appropriate program enrollment.

Program enrollment is always associated with a level of care as well as specific targeted program groups, and evidence-based services. In addition, the program will be tied to a grant if that is appropriate.

Program Setup

^ Hide Context Information

Agency Name	Facility Name	Current Enrolled	Program Type
County Assessment and Treatment Center	Fort Collins	3	Substance Use Treatment

Program Name

Display Name

Domain

Program Start Date

End Date

Modality

Modality Specifier

Level of care

Grant

Residence

Report to State
☒ Yes ☐ No

Report to TEDS
☐ Yes ☒ No

Available Reporting Guidelines

Selected Reporting Guidelines

Age Group

Gender Specific

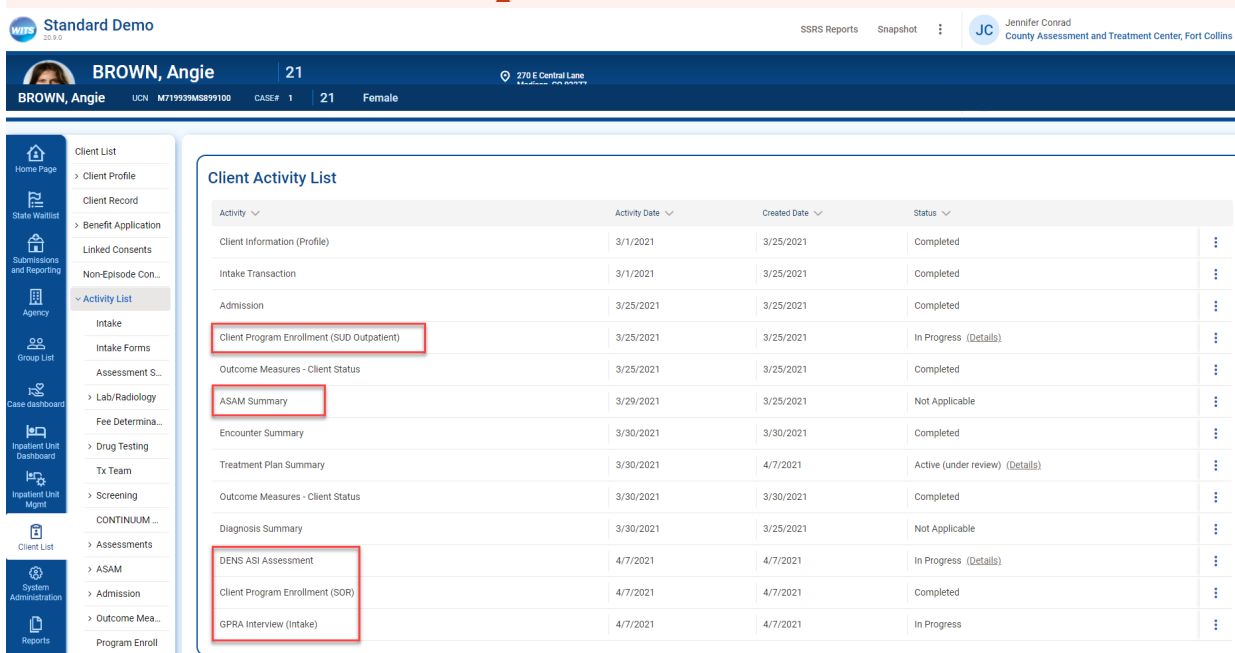
Waitlist Availability Type

Available Evidence-Based Practices

Selected Evidence-Based Practices

Exhibit 13. Program Set Up Screen Shows Grant, Level of Care and Evidence Based Practices

All clinical care items provided for the client will appear in their Client Activity list on Screen. The client Angie Brown, shown below, has received a GPRA, a DENS-ASI, and an ASAM, and all are part of her case file.



Activity	Activity Date	Created Date	Status
Client Information (Profile)	3/1/2021	3/25/2021	Completed
Intake Transaction	3/1/2021	3/25/2021	Completed
Admission	3/25/2021	3/25/2021	Completed
Client Program Enrollment (SUD Outpatient)	3/25/2021	3/25/2021	In Progress (Details)
Outcome Measures - Client Status	3/25/2021	3/25/2021	Completed
ASAM Summary	3/29/2021	3/25/2021	Not Applicable
Encounter Summary	3/30/2021	3/30/2021	Completed
Treatment Plan Summary	3/30/2021	4/7/2021	Active (under review) (Details)
Outcome Measures - Client Status	3/30/2021	3/30/2021	Completed
Diagnosis Summary	3/30/2021	3/25/2021	Not Applicable
DENS ASI Assessment	4/7/2021	4/7/2021	In Progress (Details)
Client Program Enrollment (SOR)	4/7/2021	4/7/2021	Completed
GPRA Interview (Intake)	4/7/2021	4/7/2021	In Progress

Exhibit 14. Client Activity List is tied to Client's Profile information

➡ 4.3.4.2 Ability to enter a Government Performance and Results Act (GPRA) entry record, at client intake, six-months post-intake, and at client discharge. [CRFQ 4.3.4.2]

The WITS Platform allows users to capture the GPRA at intake, six months, and client discharge. When the user needs to complete a GPRA, they will be able to search for the client they are about to work with by first name, last name, and other demographic data points. Once the desired client appears in the search results, the user will be able to navigate to the Activities page where they will be able to record the appropriate iteration of the GPRA Interview.

WITS currently contains a GPRA follow-up due screen, as well as GPRA follow up due alerts. Alerts appear on the home page; these allow the state or a provider to set up a defined "lead time" before the due date. For instance, the alert may appear a month before the six-month due date, if desired, to allow the provider time to schedule the follow up with the client.

The follow-up due screen allows each provider to see all clients who need follow up, and to filter on various search features (clients within the window, clients approaching the window, clients where the window has been missed, etc.). Each provider can see their own compliance rate for follow up against the target of 80%. The state can also monitor this dashboard and can see the overall compliance rate for the grant.

➡ Must perform nightly automated uploads of GPRA data into the SPARS. [CRFQ 4.3.4.4]

WITS uploads all completed GPRA records to SPARS on a nightly basis. FEI's involvement in programming these uploads in SPARS enables us to ensure that the GPRAs in WITS follow the same format and rules so that uploads can be done successfully and on a timely basis.

For each new grantee, FEI performs certification testing with the SPARS system. For West Virginia, this ensures that data is flowing smoothly and that SPARS has accepted West Virginia's uploads from WITS.

Once this testing is complete, FEI enables the nightly batch upload process in WITS. FEI's Support team monitors for any issues and will perform a re-upload if this occurs (in WITS history, this is common because of a time-out on the SPARS side in receipt of uploads).

West Virginia administrators will also be able to see the batch upload history, as well as any open error logs, from the WITS administrative screens.

- *Ability for multiple agencies to enter data regarding optional tracking of naloxone purchase, distribution and use. Must also provide state-level aggregate data. [CRFQ 4.3.4.5]*

Provider agencies across the state will have the ability to capture data related to the purchase, distribution, and use of naloxone. The State can identify which Agencies should have access to use the Overdose Reversal Module within WITS. Subsequently, those agencies will be able to track the related activities. All of this information is aggregated at the state level for reporting purposes.

- *Ability to generate ad-hoc reports for any data within the system. Report generation should have a web-based connection for deployment, which will allow reports to be accessed over the internet by all system users. [CRFQ 4.3.4.6]*

Non-technical users can generate ad hoc reports from WITS via access to Microsoft's SSRS, which is the primary reporting and analytics tool used in WITS. FEI allows the reports to be generated against a real-time copy of the production database, so information is always up to date, but long-running reports do not degrade performance for those using the system.

The SSRS reporting environment is SSO from WITS and uses the assigned permission of the user to determine which data is available. A provider will only be able to report on data from their own organization. However, a provider (or the state) may build a report that can be published to all providers—and each provider will only be able to see his or her own data. On the other hand, the state may build reports that allow for access across all reporting entities.

SSRS allows for the development of new ad-hoc reports or stored reports in table/matrix views; graphical views; or may include heat mapping data as well. In addition, "form letter" reports can be built and used to create mailings or other communications to individuals within the database.

Data is available in real time in the SSRS workspace or saved reports can be "subscribed" and sent to people using secure email. The state will have control over the organization of the reports in SSRS and how they are stored, as well as the people who have access to run reports, or build reports. FEI's support team provides assistance and trouble-shooting with report building as needed to the state.

- *Must perform a nightly transfer of all collected data to a State of West Virginia identified/owned SQL server in a format required by BBH. [CRFQ 4.3.4.7]*

FEI will work with the state to identify the best technical way to provide a nightly transfer of all collected data into the West Virginia identified/owned SQL server in a format required by the BBH. While the technical details for each customer are slightly different, FEI works with many states across the country to ensure nightly transfers to a data warehouse or other additional systems.

- *4.3.4.8 Timeline: Completion within twelve weeks of contract award.*

Implementation of the base SOR Module within the WITS Platform can be completed with user access provided to the state within twelve weeks of contract award, as can access to the SSRS reporting module. In most cases, FEI can complete certification testing of the GPRA upload for the State's specific Grant ID with the SPARS vendor in this timeframe, however, the SPARS vendor is an external contractor and FEI may be dependent upon their response timeframes. FEI will work with the State's IT staff to determine

the best method of data transfer to the SQL server and based on their availability and the method chosen, this may take longer than 12 weeks.

2.3.4 Deliverable 4: Prevention Module [CRFQ 4.3.5]

- *Prevention module must be designed to follow SAMHSA's Strategic Prevention Framework (SPF) model, which will allow BBH to establish prevention plans and have coalitions and other providers implement work in accordance with those plans. Module will provide a method of capturing all workflow and payment data related to services, core functions supporting treatment, prevention, and recovery services. [CRFQ 4.3.5.1]*

WITS' Prevention module was designed specifically to support each of the components of CSAP's Strategic Prevention Framework and is currently used by 13 states. The prevention modules were developed as a functional area in WITS in 2009, expanded in 2012, and feature a collaborative, workflow driven approach that allows for collection and reporting of all requirements of the SAPT block grant.

The WITS Platform is designed to collect CSAP data from each provider by making the data elements required for CSAP reporting mandatory. FEI's WITS Platform is well-suited to allow BBH to establish prevention plans and have coalitions and other providers implement work in accordance with those plans. This feature could be added to the upload process if needed. Once data is entered, WVDHHR can generate both provider- and system-level reports through SSRS. FEI has developed the standard CSAP Prevention Block Grant reports within SSRS and can enable those for WVDHHR. The framework of the CSAP data collection within WITS is contained within the prevention workflow.

WITS Prevention modules will also help West Virginia build the reporting and technical infrastructure required under the SPF. The five steps of the SPF are depicted in **Exhibit 15**, which provides a detailed breakdown of how Prevention WITS features line up with the SPF model.



SAMHSA's Strategic Framework Model

Exhibit 15. WITS Prevention Features follow the SPF Model

SPF Model	Prevention WITS Features
1. Assessment – access to data sources that may be useful in conducting a needs assessment.	Prevention WITS supports the state in the Assessment phase of the logic model by providing clear and accurate access to data on both planned and delivered prevention activities as well as the targeted individuals and risk groups.
2. Capacity – identify provider and coalition organizations and members.	Prevention WITS tracks providers and agencies who support the many facets of the prevention network at multiple levels, as well as the expected level of effort and outcomes with each of these providers.
3. Planning – strategic plans; problem statements; logic models; goals/objectives; measurement indicators and measurement tools.	Prevention WITS contains a comprehensive Planning module, which is closely tied to an Implementation module, allowing the planning, implementation, and monitoring of community based and individual based strategies.
4. Implementation – identify evidence-based programs; funding; groups for recurring services; individual participants; types of services/activities; include demographics of persons served.	The Implementation module in Prevention WITS allows the state authority to approve a plan before it can be implemented. Selected providers may then implement those plans in approved regions of the state or statewide recording necessary data elements to satisfy the SAPT block grant.

SPF Model	Prevention WITS Features
5. Evaluation – report goal progress and results.	Outcome measures and process measures are reportable for prevention services, as well as any pre and post-test results. Reporting of implemented strategies against a plan allows the state as well as individual providers to track their progress towards the goals and objectives set forth for the state as a whole. This reporting is possible through pre-built reports, as well as ad-hoc reporting services.

The Prevention Modules in WITS are flexible, in that plans may be created for the state as a whole or may be created by the state for various regions of the state. In a regional model, the state may also grant regional administrators or even regional prevention entities the rights to input the regional plans. This flexibility allows the state to better manage planning as needs and capabilities change over time.

Any plan that is input does require the approval of the state before it becomes active. Once a plan is active, the state can align various coalitions and providers with each plan. For instance, if a larger prevention specialist organization is going to serve plans in three regions of the state, and these plans are slightly different, the prevention specialist will simply choose the plan based on the region of the state they happen to be working in. This allows for all work to implement plans in communities to be tracked directly back to the plan that was approved by the state. Therefore, work against each regional plan can be tracked separately, while the state can also monitor work across the entire state.

All data input is accessible for real-time reporting, so the state can monitor activity throughout the year. This also allows the state to modify plans in the event needs change throughout a planning period. For instance, if treatment data entered into WITS indicates a sudden spike in the use of a particular drug in one area of the state, the state can view this information and make decisions about changes to its prevention strategy mid-cycle, if desired, to address that spike. All of these changes can be documented within WITS. When a plan changes, these new initiatives flow directly to the prevention specialists who are implementing in the affected communities.

➡ *Must capture all SAMHSA Substance Abuse Prevention and Treatment Community Mental Health Program Grants submission data. [CRFQ 4.3.5.2]*

The WITS system currently collects and curates the Prevention, SUD treatment, and Community Mental Health Program block grant requirements. As data is entered during the planning phase, each strategy requires entry of key data such as the Institute of Medicine (IOM) classification, evidence-based type, risk categories, and CSAP Categories, as well as estimated costs and funding sources (which can include, at the state's discretion, funding outside of the SAPT block grant).

When the strategies are implemented by providers and coalitions in the community, they collect data regarding the impacted population (by race, gender, ethnicity, and age), the time spent on each CSAP activity (filtered by the CSAP Strategy(ies) chosen in the planning process), and actual costs. Because each implementation is tied to a plan, this also automatically ties it to the IOM classification, evidence-based type, and risk categories. This structured data collection process ensures that all data can be populated to the block grant tables in SSRS for the state to use in its inputs into WebBGAS.

The WITS platform includes the ability to collect additional treatment block grant data for SUD and Community Mental Health Programs, including TEDS and the URS reporting tables. Should the state desire to use these features at a later date, FEI can provide costs for this enhancement.

➡ *Develop block grant reports in accordance with identified BBH needs to assist with federal data reporting guidelines. At a minimum, captured data will include the delivery of community-based services, services*

delivered to individuals, tracking of all funding (planned and expended) for community or individual services, and the ability to bill for individual services. [CRFQ 4.3.5.3]

The WITS platform includes SUD Prevention and block grant reports to assist with federal data reporting at a state level. FEI has already developed these reports in SSRS for the state's use but will configure them based on state policy for aggregated reporting.

WITS' features ensure efficient processes by ensuring mandatory federal reporting data is entered in real time. Captured data includes the delivery of community-based services, services delivered to individuals, tracking of all funding (planned and expended) for community or individual services, and the ability to bill for individual services. Billing for Prevention Services is provided through the integrated Contract Management module of WITS, which allows for billing of any state-controlled grant funds directly through the system. WITS also allows for external billing (Medicaid, other funding sources) and this can be added at a later date, for an additional cost, should West Virginia ever need this functionality.

WITS business rules ensure that providers enter all key data collection points required by state and federal reporting requirements, thereby reducing the administrative burden of additional/duplicate data entry by having to go back and enter data that may have been missed. This allows WV staff and providers to meet reporting threshold requirements and ensure that future grant funding requests are supported through the submission of timely data.

➡ *Module must allow State prevention staff to manage their own set of provider/coalition agencies by ensuring all data is separate from the treatment agencies in the application module. [CRFQ 4.3.5.4]*

WITS was designed to allow a state to add any providers, including prevention and coalition entities, as separate agencies within the system. This naturally ensures segregation of data between prevention and treatment agencies and their respective data sets.

➡ *Timeline: Completion within twelve weeks of contract award. [CRFQ 4.3.5.5]*

While the base Prevention features are a core part of WITS, FEI's experience with thirteen states is that these features do require analysis and configuration to meet the specific needs of each state and to be fully adopted by the Prevention provider community. Therefore, FEI has included a number of hours for requirements discussions and configurations to the prevention screens and also related prevention block grant reports. This process is estimated to take 3-5 months from the date of the contract award and will be based on the availability of prevention staff to work through these requirements meetings.

The WITS platform includes the ability to collect additional treatment block grant data for SUD Treatment and Community Mental Health Programs, including the TEDS data sets and URS reporting tables. Should the state desire to use these features at a later date, FEI can provide costs for this enhancement.

2.3.5 Deliverable 5: User and Administrative/Technical Manuals [CRFQ 4.3.6]

➡ *Vendor must provide a system User Manual and an Administrative/Technical Manual for the software system. Manuals should be made available via an electronic PDF and within the software system. The Administrative/Technical Manual should only be available in the software system to those who have an administrative-level account. [CRFQ 4.3.6.1]*

FEI will provide base documentation for all functionality within the system as it is configured for West Virginia. This information is presented from a workflow orientation for various types of users, which allows users to easily understand how the system screens fit into their daily activities. Typically, this documentation includes flow charts and quick tips, as well as smart guides on the screens covered during the training. These documents will become the property of West Virginia, which may distribute them to users, post them online, or include policy or other decisions pertaining to user practice in them. The

Administrative guide will be made available to post within the software on pages that are inaccessible to End Users who do not have Administrative roles in the system.

FEI typically provides documentation in the following forms:

- [WITS Basics User Guide](#) – All users receive a WITS Basics User Guide. This document details basic navigation features, system conventions, screen formations, hints, and login information that help acclimate users to the WITS Platform.
- [WITS Administrator User Guide](#) – This extensive document provides step-by-step instructions for the management of the WITS Platform. The WITS Administrator User Guide outlines in detail the processes involved in the set-up structure for the agencies using WITS, as well as staff set up and vocabulary management features and contract billing features.
- [WITS End User Guides](#) – FEI will create one or more overall end-user guides that will contain step-by-step instructions that inform users of the specific actions and workflows within each WITS module: SOR, Prevention, ASAM, and Waitlist. The end user guide may also be split into separate stand-alone documents, focused on each subject area of the system or each type of user and their specific workflows.
- [SSRS User Guide](#) – SSRS is an ad hoc drag-and-drop reporting system that allows non-IT users to build their own reports using the names of screens and fields that they see in the system. Users do not have to have an IT background to build reports or access data. FEI will provide West Virginia with an overall user guide for SSRS, including management of the report viewer, and instructions on creating datasets and reports within SSRS Report Builder. This guide also links to several external resources that provide further in-depth education on the use of SSRS.

➡ [Timeline: Completion within twelve weeks of contract award. \[CRFQ 4.3.6.2\]](#)

User guides for ASAM, SOR, and Waitlist features will be completed within twelve weeks of contract award. Prevention training guides will be available after completion of the programming and testing of the Prevention configuration.

2.3.6 Deliverable 6: Training [CRFQ 4.3.7]

- ➡ *Vendor must provide trainings as outlined in Attachment 2. All trainings must be conducted via interactive, live webinar due to the COVID-19 pandemic, except as noted for the ASAM CO-Triage® Training, which is an established, online course. The BBH will provide the vendor with a list of individuals who will receive the trainings. In the event that any on-site training was to be conducted, vendor would be responsible for all costs incurred for travel for staff attending the training and installation. [CRFQ 4.3.7.1]*

As part of our standard implementation offering, FEI is practiced at leading virtual training sessions. FEI's training team will provide all training related to the WITS system. To support the implementation of ASAM's CONTINUUM and CO-Triage tools, FEI has partnered with the ASAM Education team to deliver training as outlined in Attachment 2 of the CRFQ.

The training approach consists of a virtual classroom type setting using Zoom or GoToTraining where training will be provided, and end users are walked through the application step-by-step. Virtual training allows for users to ask questions, answer poll questions, and interact with the trainer to troubleshoot issues by sharing screens. This is typically facilitated by a lead instructor and one assistant to manage the chat and answer questions. Attendees should be familiar with PCs and internet browsers before attending training. In addition, users will need to have a stable internet connection to attend the training.

Exhibit 16 includes the number of training that FEI and ASAM have included in the pricing, for each type of feature. In some cases, FEI has estimated the number of users (for instance, for SOR, waitlist, or prevention). While the number of users of these features does not impact the pricing of the system, it

could alter the required number of training sessions. In addition, FEI and ASAM are currently assuming that training will be performed virtually.

Exhibit 16. Planned Training Sessions

Type of Training	# of Sessions	MAX # Attendees per session	Length of Time	# of Trainers
WITS State Administrator/ SSRS Training	1	20	8 hours	2 FEI Trainers
WITS State Administrator Training Prevention/ SOR & GPRA	1	20	8 hours	2 FEI Trainers
ASAM Criteria Training	5	105*	8 hours	2 ASAM Trainers
ASAM Continuum Training	5	105*	8 Hours (2 hours WITS, 6 Hours Continuum)	2 FEI Trainers 2 ASAM Trainers
ASAM Co Triage/WITS	1	40	1.5 hours	2 FEI Trainers
ASAM Online Training Module	-	40	-	Web-Based
SOR/GPRA End User Training	2	25	2 Hours	2 FEI Trainers
Waitlist End User Training	2	40	2 Hours	2 FEI Trainers
Prevention Coordinator Training	1	30	8 Hours	2 FEI Trainers
Prevention End User Training	5	25	4 Hours	2 FEI Trainers

*ASAM is willing to honor its previous commitment to West Virginia to train 100 users per session; however, recent changes in training performed by ASAM show that 75 participants is a better cap for this type of training.

➡ **Timeline:** *Completion within sixteen weeks of contract award. [CRFQ 4.3.7.2]*

Virtual training can be completed within sixteen weeks of contract award. FEI will work with ASAM's organization training staff to ensure that training for all providers using the system can be presented in a coordinated fashion, to as much an extent possible. Given the summer holidays and large time commitment for ASAM training, this may extend beyond the 16 weeks.

Prevention training can be scheduled and completed within two weeks after the Prevention modules have been configured and moved to the training site for West Virginia.

2.3.7 Maintenance, Support, and Upgrades [CRFQ 4.3.8]

➡ *Vendor will provide software, software support, and software licenses to all identified users, including WVDHHR central office users. Vendor will support its use Monday through Friday 8:00 am to 5:00 pm Eastern Standard Time, including State holidays. [CRFQ 4.3.8.2]*

FEI provides all software and necessary CONTINUUM subscriptions to identified users, and those have been included in our cost proposal. WITS functionality does not require a license. The budget proposal includes FEI providing ongoing Tier 3 support to WVDHHR central office users. Tier 1 support is generally provided at the provider organization level, and Tier 2 support is generally provided by the customer (i.e., BBH) or another contracted agency.

The FEI Help Desk team is available Monday through Friday, 8:00 a.m. to 8:00 p.m. ET, excluding some federal holidays. After-hours support is available 24/7/365 days per year to address production environment outages. FEI's trained and experienced Help Desk team is responsible for the following:

- Coordinating with BBH's Tier 2 support to understand and further document all reported issues
- Performing detailed analysis of the issue, working with the appropriate development team members when needed
- Determining the appropriate course of action to mitigate the issue
- Assigning priority for bug fixes
- Helping with data corrections
- Helping the state with SSRS reports

- Running audit reports
- Providing monthly uptime reports
- Escalating environment related issues for immediate resolution

In addition to the above, FEI’s ongoing support includes an Account Manager, who meets regularly with the State to support the use of the system. It also includes participation in the WITS User Group Meetings.

FEI responds to and resolves problems reported during normal business hours. All issues reported during normal business hours are resolved based on FEI’s Standard Service Level Agreements (SLAs).

FEI’s pricing proposal assumes that FEI will provide Tier 3 support to the State, meaning that the State will appoint administrators who will notify FEI if any user issues require FEI’s intervention. This proposal also assumes that FEI will triage any clinical ASAM questions to the ASAM organization and includes pricing for ASAM’s clinical support desk staff to answer these questions.

Tier 2 support services—specifically help desk support to provider organizations—can be available to BBH either for a short time period (e.g., during onboarding) or ongoing. FEI will provide BBH with a cost proposal for Tier 2 support upon request.

- *Vendor must perform daily system monitoring, with reporting and resolution of anomalies. Issues and anomalies should be reported directly to the identified BBH staff person (to be identified upon contract award) via email. [CRFQ 4.3.8.3]*

FEI monitors its systems infrastructure health and utilization using a variety of tools, including SolarWinds for network monitoring and Microsoft Systems Center Operations Manager. The FEI thresholds and trigger alarms alert the FEI IT team any time action needs to be taken. In the event of an outage, FEI will report that information directly to the identified BBH staff person. **Exhibit 17** is a sample report from SolarWinds.

WITS Up-Time Report	
Summary of Orion Objects: WITS PROJECT NODES	
Summary of Time Periods: Last 12 Months (Mar 1 - Feb 29, 2016)	
WITS Nodes Availability for WITS PROJECT NODES from Last 12 Months (Mar 1 - Feb 29, 2016)	
LIFECYCLE	AVERAGE AVAIL
September 2015	
PRD	100.00 %
October 2015	
PRD	99.40 %
November 2015	
PRD	99.92 %
December 2015	
PRD	99.99 %
January 2016	
PRD	99.99 %

Exhibit 17. SolarWinds Sample Report

FEI also monitors SPARS uploads and receives email notifications if a SPARS upload fails or a file is rejected. In the event that occurs, the FEI Help Desk team will notify the proper BBH staff person.

- *Vendor must host all system hardware, software, and all data. [CRFQ 4.3.8.4]*

FEI delivers a secure hosting environment for all hardware, software, and data. Through our facilities and associated FEI-operated infrastructure, FEI provides full Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) services for more than 45 customers, including federal agency clients, numerous states,

large counties, and private industry. Our solutions are protected through a comprehensive set of security and privacy capabilities. As a national healthcare IT provider, FEI is subject to a comprehensive body of regulatory mandates regarding security controls.

- *As needed, vendor will troubleshoot anomalies, either independently or working with a current SAMHSA contractor. [CRFQ 4.3.8.5]*

FEI provides defect fixes on all new development authorized by BBH, as well as any defects found by other customers in common modules. All defects and issues are reported to the FEI Help Desk via phone, email, or through the built in Support Ticket module within WITS. The FEI Help Desk staff logs the defect within Ivanti as a help desk ticket and the ticket number is provided to BBH. Upon confirmation that the reported issue is a defect, a work item number is provided to BBH along with the assigned severity. All Critical and High severity bugs are fixed in a maintenance or branch release. Medium and lower severity bugs are fixed in the next appropriate release.

- *Vendor will provide ongoing 24/7/365 support services for addressing data errors, hardware issues, and system availability. [CRFQ 4.3.8.6]*

The FEI Help Desk is the first point of contact and coordinating entity for all system related questions and issues.

- FEI Help Desk team is available Monday through Friday, 8:00 a.m. to 8:00 p.m. ET, excluding some federal holidays
- After-hour support is available 24/7/365 days per year to address production environment outages

- *Vendor must provide online training and technical assistance on the web-based data collection system as outlined in Deliverable 6 and Attachment 2 for the entirety of the contract. Vendor must maintain HIPAA compliance with all data and provide a back-up of the data offsite to prevent loss of data integrity. [CRFQ 4.3.8.7]*

FEI provides online training and technical assistance on the web-based data collection system as outlined in Deliverable 6. All training materials may be linked to the WITS front end so that they are easily accessed by users as needed at any point in time. Any additional training sessions after go-live can be estimated and planned through FEI's Change Management process.

FEI uses an Equinix Internet Business Exchange Data Center in Ashburn, Virginia, and a backup hosting facility in Austin, Texas. To achieve optimal redundancy most effectively, system components are hosted across three virtual machine clusters in the two geographically separate data centers. The two clusters in the Virginia location host the system during normal operation. Intra-cluster failover is provided through local cluster mechanisms, whereas inter-cluster failover is provided through system native components, such as load balancing or database failover. To ensure complete redundancy, nodes for each component are implemented on each cluster. The third cluster is at the Austin, Texas, data center, which acts as a Disaster Recovery site.

As the data processed in the system contains PHI/PII, all backup target locations and transmitted data associated with backups is encrypted. FEI uses Rubrik, an integrated SLA policy-driven backup and recovery platform, to manage and operate system backups. Additionally, Storage Area Network (SAN)-based snapshots are used for full virtual machine (VM)/operating system (OS) level backups. FEI leverages Microsoft Azure for long term backup retention. SSL-encrypted connections carry backup data transmissions, which also leverage FIPS 140-2 compliant algorithms. As part of HIPAA compliance, FEI's long term backup retention extends to six years, with daily backup retention exceeding the 30-day requirement.

- *Vendor must provide support services (for the duration of the contract) for network management, database management and security management including pro-active monitoring of system where appropriate. [CRFQ 4.3.8.8]*

For all hosted customers, FEI has established a routine maintenance window on the third Saturday of each month, from 6:00 a.m. to 12:00 p.m. ET. FEI uses this window to apply Windows updates and patches, to reconfigure or apply changes to firewalls, to perform database maintenance (such as re-indexing), and to migrate to new web and LDS (authentication) servers. FEI also uses this window to perform tasks necessary to maintain integrated failover and Disaster Recovery capabilities in a secondary secure site, located in a different section of the country than the primary secure hosting site. FEI's Help Desk sends a reminder to all customers each month before the maintenance weekend and sends an email when the maintenance is complete.

- *Vendor must continually upgrade system to maintain data collection, ASAM Criteria, reporting of federal GPRA, block grant, and Medicaid 1115 Waiver requirements, and other needs as identified by BBH. [CRFQ 4.3.8.9]*

As necessary, FEI modifies WITS to be compliant with federal TEDS reporting, as well as SAPT Block grant reporting standards. ASAM criteria updates are provided by FEI as required by ASAM, pursuant to the contract FEI holds with ASAM as an organization. FEI will provide up to 80 hours of enhancement work for changes related to Federal Government requirements. These incremental changes are usually small and shared by many customers. For larger changes in the healthcare industry (i.e., Interface Control Document (ICD)-9 to ICD-10 or HIPAA 4010 to 5010 X12 standards), the cost of the enhancement will be shared amongst the WITS customer base. With this model, the State can get new functionality at a fraction of the cost of developing a "from scratch" solution. Due to our relationships with federal data collection and reporting contracts, FEI is in a unique position to remain aware and prepare for upcoming federal reporting requirements.

The proposed pricing for West Virginia includes Prevention Block Grant reporting as requested in the CRFQ. Additional treatment block grant reporting for SUD and mental health can be added if desired as a later scope of work.

- *Vendor shall provide within the system: a) System User Manuals and b) System Administrator/Technical Manuals. Manuals must be available within eight weeks of contract award. [CRFQ 4.3.8.10]*

The system allows BBH to link to help documents, videos, or diagrams particular to the context of a module, as shown in **Exhibit 18**. When help is available on a particular screen or module, the user sees a Help option in the top header bar. As long as the link remains the same, the user can see the newest version as help documents and/or videos are updated.

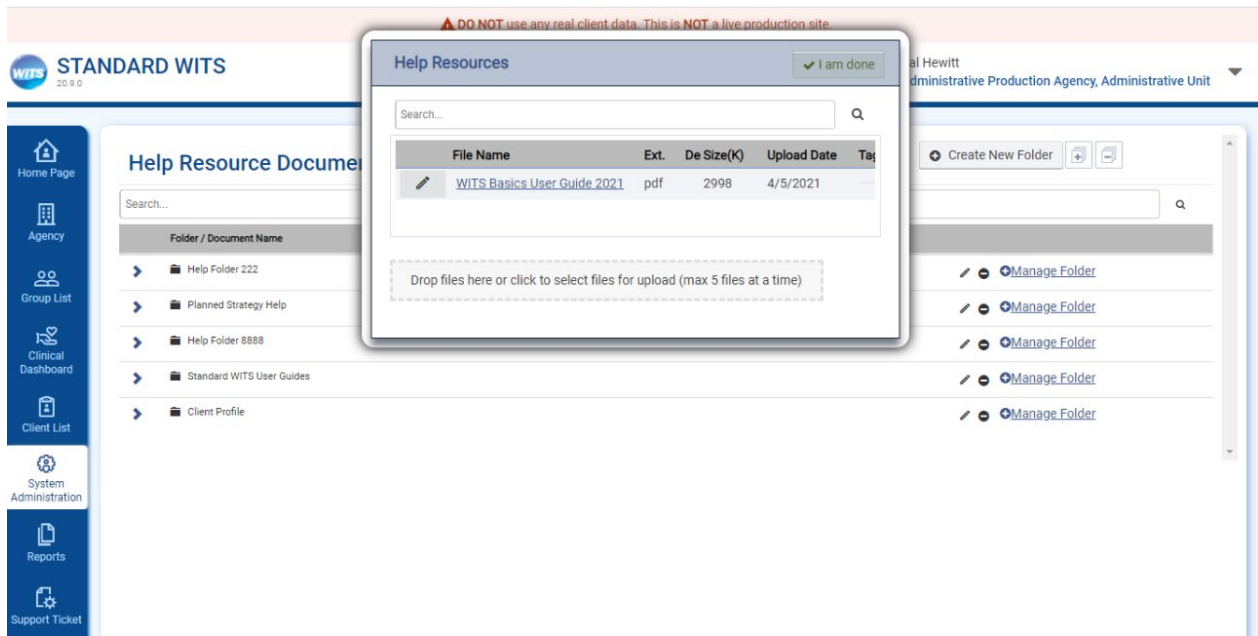


Exhibit 18. Help Resources File Upload Window

FEI will provide the user manuals within twelve weeks of award, as requested in Section 2.3.5 of this response. The Prevention user manuals will be provided upon completion of the Prevention configuration work as discussed in this response. System User Manuals and System Technical Documentation, as required by the System Administrators, will be provided to the State administrators during the planned State Administrator training, and will show details on the features that can be performed by the State administrators.

➡ *For the duration of the contract and eventual updates, vendor must ensure continuing hardware and software compatibility to avoid data loss, functionality loss, or usability issues. [CRFQ 4.3.8.11]*

WITS is built on a Service Oriented Architecture (SOA) that is highly scalable and load-balanced over multiple logical or physical servers within or across network domains. This application-level redundancy, combined with redundancy at the physical layer within FEI's private cloud offering, enables FEI to achieve BBH's system availability requirements. The combination of hardware redundancy, load-balancing infrastructure, site configuration, and application design ensures the system remains accessible to BBH stakeholders. **Exhibit 19** describes the layers and approach to redundancy.

Exhibit 19. FEI Hosting Redundancy Approach Promotes System Availability

Layer	Redundancy Approach
External Connectivity	Redundant internet connections with automated failover using Border Gateway Protocol
Firewalls	Clustered firewalls
Network	Redundant switches and connectivity to multiple switches
Hosts	Fully virtualized infrastructure with host migration capabilities if there is a node hardware failure
Storage	Mirroring and Redundant Array of Inexpensive Disks (RAID) disk protection, along with redundant controllers and paths to disks
Web Layer	Load balanced web servers that are stateless
Application Layer	Load balanced application servers
Database Layer	SQL Always-On redundancy along with database replication
System Layer	Two fully independent virtual host clusters; All load balanced components are split between these two clusters (one node on each).

Layer	Redundancy Approach
Application Integration and Jobs	Scheduled jobs and integration services are built with custom verification processes to ensure success. In many cases, retries and re-execution are automated through the verification processes.

3 Miscellaneous – Contract Manager [CRFQ 9; CRFQ 9.1]

FEI has named an Account Manager who will manage all aspects of the relationship, including contractual, during the life of the contract.

Contract Manager: Erin Leatherwood

Telephone Number: (443) 518-7266

Fax Number: (410) 715-6538

Email Address: Erin.leatherwood@feisystems.com



WITS Master License Agreement

This WITS MASTER LICENSE AGREEMENT (this “Agreement”) is entered into and effective as of the ___ day of _____ by and between **FEI.com, Inc., a Maryland corporation d/b/a FEI Systems having its principal offices at 9755 Patuxent Woods Drive, Suite 300, Columbia, Maryland 21046** (hereinafter referred to as “Licensor”) and **[INSERT COMPANY NAME]**, a governmental agency with its principal offices at **[INSERT COMPANY ADDRESS ADDRESS]** (hereinafter referred to as “Licensee”).

WHEREAS, Licensor is, among other things, a software developer with expertise in developing computer software and systems to be used by various governmental agencies and entities for purposes of interfacing with the U.S. federal government’s treatment services system.

WHEREAS, Licensee is desirous of licensing and using Licensor’s software to be used in connection with Licensee’s treatment services system.

THEREFORE, pursuant to the terms and conditions contained herein and any attachments hereto, and for consideration of the mutual covenants and agreements herein contained and for other good and valuable consideration, receipt of which is hereby acknowledged, the parties, intending to be legally bound, hereby covenant and agree as follows:

1. Definitions.

- 1.1. The term “Core Software” shall mean the proprietary software co-authored, co-developed, and co-owned by Licensor and the University of Maryland Bureau of Governmental Research (“BGR”) prior to the Effective Date which provides “core” functionality to and is integral in the use and operation of the Licensed Software.
- 1.2. The term “Developed Module(s)” shall mean one or more pieces of software created by Licensor at the request of one or more third parties (including but not limited to Licensor and BGR) which, when used with the Core Software, add functionality and utility to the Licensed Software. The Developed Modules in existence as of the Effective Date are listed on Schedule A, attached. For purposes of clarity, “Developed Module(s)” includes the Custom Developed Modules and Future Developed Modules.
- 1.3. The term “Licensed Software” shall mean the executable software application known as the Web Infrastructure for Treatment Services Systems (“WITS”), consisting of the Core Software, FEI Software Modules, Developed Modules, and other modifications to the Licensed Software from time to time made by Licensor, but specifically excluding such modifications related to the addition of enhancements to the software which are not necessary to the basic functions of the software, and which are not related to the repair of bugs or errors in, the software.



WITS Master License Agreement

- 1.4. The term "Scope of Work" shall mean that certain document entitled "Scope of Work" entered into by and between the parties separate from this Agreement, which sets forth the commercial terms relating to services (including but not limited to design, development, programming, implementation, and support services) associated with the Licensed Software. The Scope of Work may make reference to but will not be made a part of this Agreement.
- 1.5. The term "Custom Developed Module(s)" shall mean one or more Developed Modules created by Licensor for Licensee pursuant to the Scope of Work.
- 1.6. The term "Future Developed Module(s)" shall mean Developed Module(s) not in existence as of the Effective Date but which come into existence at some future date.
- 1.7. The term "Effective Date" shall mean the date this Agreement is signed by both parties, or at a later date specified in the Agreement once that date has arrived or passed.
- 1.8. The term "FEI Software Module(s)" shall mean one or more pieces of software created by Licensor, independently and/or using its own funds, and offered by Licensor, at its sole discretion, as a part of the Licensed Software, including without limitation, derivative works of Custom Developed Modules and Developed Modules created by Licensor, independently and/or using its own funds.

2. Grant of License.

- 2.1. In consideration of the certain license back from Licensee and other consideration hereunder, Licensor grants to Licensee a non-exclusive, perpetual, royalty free, fully paid license to use the Licensed Software in executable form, together with any and all related documentation, manuals, or instructions, either in hard copy or electronic form, subject to and in accordance with the terms and conditions of this Agreement, such software to be used for solely for the purposes of operations of Licensee's organization in connection with Licensee's treatment services and/or transfer of data relating to such treatment services.
- 2.2. Licensee shall have the right to permit its agency, departments, staff within Licensee's organization and Licensee's third party treatment services system providers to use the Licensed Software solely for the purposes of operations of the Licensee's organization in connection with Licensee's treatment services, consistent with the terms of this Agreement.



WITS Master License Agreement

- 2.3. It is understood by the parties that Licensee may choose to use as many or as few of the Developed Modules as it may desire, and Licensee may add or eliminate Developed Modules from its implementation of the Licensed Software at any time.
- 2.4. During the term of this Agreement, the Licensee shall be entitled to receive from Licensor, at no additional charge to Licensee, all upgrades and revisions to the Licensed Software as determined by Licensor to be necessary for the repair of errors or omissions, including but not limited to software bugs.
- 2.5. Upon Licensee's written request to Licensor, Licensee shall be entitled to have access to and use of the source code for the Licensed Software (but specifically excluding the FEI Software Modules) for maintenance, upkeep, and continued private development purposes only. Upon termination of this Agreement, so long as Licensee is not in breach of its confidentiality and intellectual property obligations hereunder, Licensee shall have use of the source code of the Licensed Software (but specifically excluding the FEI Software Modules) which was available up to the time of termination in perpetuity. Notwithstanding any other provision in this Agreement, so long as the Licensee is in possession of any such source code related to the Licensed Software, Licensee agrees to take reasonable efforts to protect the secrecy and confidentiality of the source code and shall not disclose the source code to anyone without the prior written consent of Licensor, at its sole discretion. In the event that Licensee desires to access and use the source code for the FEI Software Modules, such access and use shall be subject to the terms and conditions and fees in accordance with Licensor's then-current license agreement for the source code for the FEI Software Modules.

3. License Back

- 3.1. Licensee grants to Licensor an exclusive license to use, install, modify, make derivative works of, offer for sublicense, and sublicense any Custom Developed Module(s) created by Licensor for Licensee, together with any and all related documentation, manuals, or instructions, either in hard copy or electronic form at no cost/fee. Subject to the terms and conditions hereunder, Licensor agrees to take reasonable efforts to protect the secrecy and confidentiality of the Licensee's source code to the Custom Developed Module(s).
- 3.2. Licensor shall not be required to provide an accounting for or pay royalties to Licensee for any licenses, sublicenses, or other uses of the Custom Developed Module(s) or modifications, improvements or derivative works thereof which are provided to Licensor's licensees.

WITS Master License Agreement

- 3.3. For purposes of clarity, Licensor shall have the right, among other things, to use and modify the source code to the Custom Developed Module(s) for purposes of enabling the Custom Developed Module(s) to be used by third-party licensees or sublicensees of Licensor in connection with past or future licenses of the Licensed Software, subject to the obligations of confidentiality contained hereunder.
- 3.4. The obligations under this Section shall survive the termination of this Agreement.

4. Option to License Future Developed Modules.

- 4.1. From time to time during the term of this Agreement, Licensor may, at its sole discretion, inform Licensee of the existence of Future Developed Modules not in existence as of the Effective Date. Licensee shall have, at its sole discretion, the option to license such Future Developed Modules in accordance with the terms contained herein.
- 4.2. If Licensee shall desire to incorporate such Future Developed Modules into the Licensed Software, Licensee shall advise Licensor in accordance with the notice provisions hereunder, and those Future Developed Modules shall thereafter be made available to Licensee for installation and incorporation into the Licensed Software, and the identity of such Future Developed Modules shall be added to Schedule A by written amendment executed by both parties, thereby becoming part of the Licensed Software as of the date of such written amendment.
- 4.3. If Licensee elects to incorporate Future Developed Modules into the Licensed Software, there shall be no additional charge for such modules. Licensee and Licensor may separately negotiate a cost for any software configuration, customization, or installation services which may be required or requested.

5. Use of the Licensed Software.

- 5.1. Licensee agrees to take all reasonable steps to ensure that all of its employees, contractors, officers, and agents using the Licensed Software are familiar with and abide by the terms and conditions of this Agreement.
- 5.2. Licensee shall, at Licensee's sole cost and expense, purchase and provide the necessary operating system software, computer hardware, and computer-machine interface hardware required, specifications for such hardware and software requirements to be provided by Licensor.



WITS Master License Agreement

- 5.3. Licensee agrees that it shall not attempt to reverse engineer, reverse compile, or disassemble the computer code (or any trade secrets or algorithms embodied therein) of the Licensed Software.

6. Maintenance and Support.

- 6.1. Licensors shall not be obligated to provide any maintenance or support services to Licensee under this Agreement. Any maintenance and support services relating to the Licensed Software shall be set forth and governed by either the Scope of Work or a services agreement to be separately entered into by and between the parties.

7. Documentation and Manuals.

- 7.1. Licensors may, but shall not be obligated to, produce documentation and written instructions reasonably calculated to instruct and enable Licensee to use and take advantage of the full functionality of the Licensed Software (the "Maintenance Manual"). The Maintenance Manual may be supplied to Licensee by Licensors in a form accessible to Licensee (electronic or hard copy form). The Maintenance Manual may be updated periodically by Licensors, at no additional cost to Licensee, as upgrades, revisions, or other material changes or modifications are made to the Licensed Software, such updates also to be provided in electronic or hard copy formats.

8. Term and Termination.

- 8.1. This Agreement shall commence on the Effective Date and shall continue in effect thereafter until and unless terminated in accordance with this Section.
- 8.2. Licensee may terminate this Agreement upon thirty (30) days' prior written notice to Licensors if Licensors fails to comply with any of the material terms and conditions contained herein and if such failure to comply is not corrected within such thirty (30) days from the date of Licensee's written notice of termination to Licensors ("Termination For Cause by Licensee"). In the event of Termination For Cause by Licensee, all rights, duties, and obligations of Licensors and Licensee under this Agreement shall cease except as otherwise expressly provided hereunder.
- 8.3. Licensors may terminate this Agreement upon thirty (30) days' prior written notice to Licensee if Licensee fails to comply with any of the material terms and conditions contained herein and if such failure to comply is not corrected within such thirty (30) days from the date of Licensors's written notice of termination to Licensee ("Termination For Cause by Licensors"). In the event of Termination



WITS Master License Agreement

For Cause by Licenser, all rights, duties, and obligations of Licenser and Licensee under this Agreement shall expressly cease except as otherwise provided hereunder.

- 8.4. Either the Licensee or Licenser may cancel this Agreement at any time, with or without cause, upon thirty (30) days' prior written notice to the other party specifying the date of termination.

9. Ownership and Derivative Works.

- 9.1. Licenser represents and warrants that it has the full right and authority to license the Core Software and the FEI Software Modules for use by Licensee in connection with the Licensed Software. Licenser represents and warrants that it has the full right and authority to license any Custom Developed Modules and Future Developed Modules for use by Licensee in connection with the Licensed Software.
- 9.2. The Core Software and all related documentation, manuals, and instructions are protected by applicable copyright, patent, trademark, or trade secret laws. Licensee acknowledges that Licenser and the co-creator of the Core Software own all right, title and interest in and to the Core Software. Licensee agrees to take any reasonable steps necessary to protect the proprietary rights of Licenser and to avoid the infringement, direct or indirect, of such rights.
- 9.3. The FEI Software Modules and all related documentation, manuals, and instructions are protected by applicable copyright, patent, trademark, or trade secret laws. Licensee acknowledges that Licenser owns all right, title and interest in and to the FEI Software Modules. Licensee agrees to take any reasonable steps necessary to protect the proprietary rights of Licenser and to avoid the infringement, direct or indirect, of such rights.
- 9.4. The Custom Developed Modules and all related documentation, manuals, and instructions are protected by applicable copyright, patent, trademark, or trade secret laws. Licenser acknowledges that Licensee owns all right, title and interest in and to the Custom Developed Module(s). Licenser shall have the right to use the Custom Developed Module(s) as provided herein. Licenser agrees to take any reasonable steps necessary to protect the proprietary rights of Licensee and to avoid the infringement, direct or indirect, of such rights.
- 9.5. The obligations under this Section shall survive the termination of this Agreement.



WITS Master License Agreement

10. Confidentiality.

- 10.1. Except as prohibited by law or in contravention of applicable law or regulation, the parties to this Agreement agree to maintain all of the terms of this Agreement, any Exhibits, and any attached Addenda, as well as the substance of any discussions, negotiations, and correspondence related to this Agreement in strict confidence, and to keep same from any and all third parties, except such disclosures that are otherwise required by law. In the event of such disclosures, the disclosing party agrees to provide the other party advance notice of its intention to provide such disclosures, including with such notice the name and contact address and telephone number of the entity to whom such disclosures shall be made.
- 10.2. Except as prohibited by law or in contravention of applicable law or regulation, the parties to this Agreement shall make reasonable efforts and use reasonable care to protect the secrecy of all trade secrets and confidential and proprietary information and documents related to the other party, including without limitation, the Licensed Software and its source code (“Confidential Information”). Notwithstanding the foregoing, Confidential Information does not include information which: (i) was publicly known or generally known within the trade at the time of disclosure, (ii) becomes public knowledge or generally known within the trade without breach of this Agreement by either party or any of its directors, officers or employees, (iii) was information already known by the receiving party at the time of disclosure, or information independently developed by the receiving party’s personnel who did not have access to the information disclosed by the disclosing party, (iv) is required to be disclosed by law, or (v) is obtained by the receiving party, its officers or employees from third parties who are under no obligation of confidentiality with respect to the information. If the receiving party is required to disclose any Confidential Information by a court order or other specific governmental action, the receiving party may comply with such disclosure requirement, unless the disclosing party, at its own expense, is successful in having the effect of such requirement stayed pending an appeal or further review thereof, or revised, rescinded or otherwise nullified. In all events, the receiving party agrees to notify the disclosing party promptly if at any time a request or demand of any kind is made to the receiving party to disclose any of the Confidential Information. The disclosing party shall have the right, at its cost, to intervene in any proceeding in which the receiving party is being asked to disclose any of the Confidential Information.
- 10.3. The obligations of secrecy and confidentiality contained in this Section shall be in effect during the term of this Agreement and shall survive termination and



WITS Master License Agreement

remain in effect for a period of five (5) years after termination of this Agreement.

11. Infringement.

- 11.1. Licensor represents and warrants that Licensor has all right to furnish the Licensed Software in accordance with the terms and conditions of this Agreement and that the Licensed Software and Licensee's use thereof do not and shall not directly or indirectly violate or infringe upon any copyright, patent, trademark, trade secret, or other proprietary or intellectual property right of any third-party. Licensor shall indemnify and hold Licensee and its successors, officers, directors, employees, and agents harmless from and against any and all actions, claims, losses, damages, liabilities, awards, costs, and expenses (including reasonable attorneys' fees and costs) resulting from or arising out of any breach or claimed breach of the foregoing warranty of non-infringement and Licensor shall defend and settle, at its sole expense, all suits or proceedings arising therefrom.
- 11.2. Licensee shall immediately inform Licensor of any suit or proceeding against Licensee for which indemnity is claimed under the foregoing warranty of non-infringement. Licensee shall have the right to participate in the defense of any such suit or proceeding, at its own expense and through counsel of Licensee's choosing, but may not impede or hamper Licensor's defense of or efforts to settle any such suit or proceeding. Licensor shall have the sole right to conduct the defense of any such suit or proceeding and all negotiations for its settlement or compromise, unless otherwise mutually agreed to in writing between the parties hereto. Licensor shall notify Licensee of any actions, claims, or suits against Licensor based on an alleged infringement of any party's intellectual property rights in and to the Licensed Software.
- 11.3. Licensor shall have no obligation in any respect for any claim based on (A) Licensee's unauthorized or permitted modification of the Licensed Software, as delivered by Licensor, or its combination, operation, or use with any product, data, or apparatus not specified or provided by Licensor, provided that such claim solely and necessarily is based on such combination, operation, or use and such claim would be avoided by combination, operation, or use with products, data, or apparatus specified by Licensor, or (B) use of any releases other than a current release or one (1) prior release of the Licensed Software if such claim would have been avoided by use of a current release or prior release.
- 11.4. The obligations under this Section shall survive the termination of this Agreement.



WITS Master License Agreement

11.5. THIS SECTION STATES LICENSOR'S ENTIRE OBLIGATION TO LICENSEE WITH RESPECT TO ANY CLAIM OF INFRINGEMENT. ANY AND ALL OTHER EXPRESS OR IMPLIED WARRANTIES OF NON-INFRINGEMENT ARE EXPRESSLY AND SPECIFICALLY DISCLAIMED.

12. Limited Warranties.

- 12.1. Licensor warrants that, for a period of ninety (90) days following delivery, the Licensed Software will operate in all material aspects in accordance with the Scope of Work and any documentation, instruction, directions, or manuals provided by Licensor to Licensee when the Licensed Software is used in accordance with the uses described in the Scope of Work and any documentation, instructions, directions, or manuals.
- 12.2. Licensor warrants that, at the time the Licensed Software is provided to Licensee, no portion of the Licensed Software shall contain any "time bomb," "Trojan horse," "worm," "drop dead device," "virus," or other routine, device, or undisclosed feature designed to (i) disable, damage, or erase the Licensed Software or any portion thereof or any other data, or (ii) perform any similar actions that would preclude full use of and access to the Licensed Software by the Licensee.
- 12.3. Licensor warrants that it has the right to grant a license for the use of the Licensed Software.
- 12.4. LICENSOR DISCLAIMS ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, WRITTEN OR ORAL, IN CONNECTION WITH THE LICENSED SOFTWARE, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF TITLE, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. EXCEPT FOR ANY EXPRESS WARRANTIES STATED IN THIS AGREEMENT, IF ANY, THE LICENSED SOFTWARE IS PROVIDED WITH ALL FAULTS, AND THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY, AND EFFORT IS WITH THE LICENSEE.
- 12.5. LICENSOR EXPRESSLY DISCLAIMS ANY WARRANTY OR REPRESENTATION TO ANY PERSON OTHER THAN LICENSEE WITH RESPECT TO THE LICENSED SOFTWARE OR ANY PART OF IT. THIS AGREEMENT IS NOT INTENDED TO CONFER ANY RIGHTS TO ANY THIRD PARTY BENEFICIARY, AND ONLY LICENSOR AND LICENSEE HAVE THE RIGHT TO ENFORCE ANY OF THE TERMS HEREIN. ANY AND ALL EXPRESS OR IMPLIED WARRANTIES ARE EXPRESSLY AND



WITS Master License Agreement

SPECIFICALLY DISCLAIMED BY LICENSOR AND WAIVED BY LICENSEE.

13. Limitation of Liability.

- 13.1. For purposes of clarity, Licensor has no obligation in respect to any claim arising out of Licensee's unauthorized or permitted modifications to the Licensed Software or its combination, operation, or use with any product, data, or apparatus not specified or provided by Licensor at the time of delivery.
- 13.2. IN NO EVENT SHALL EITHER PARTY BE LIABLE, ONE TO THE OTHER, FOR INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF PROFITS, REVENUE, DATA, OR GOODWILL, BUSINESS INTERRUPTION, OR FOR LIABILITY TO THIRD PARTIES, ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR THE FURNISHING, PERFORMANCE, OR USE OF THE LICENSED SOFTWARE (OR ANY PART THEREOF) PROVIDED FOR IN THIS AGREEMENT, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES.

14. Relationship of the Parties.

- 14.1. This Agreement is not intended to constitute, create, give effect to, or otherwise recognize a joint venture, partnership, or formal business entity of any kind, and the rights and obligations of the parties shall be limited to those expressly set forth herein. Nothing herein shall be construed as an obligation or be deemed to obligate the parties to enter into any future agreement with respect to the matters set forth in this Agreement or as providing for the sharing of profits or losses arising out of the efforts of either or both parties. Each party shall act as an independent contractor to the other and not as an agent of the other for any purpose whatsoever and neither party shall have any authority to bind the other or enter into any agreement on behalf of the other.

15. Construction.

- 15.1. The parties each warrant and acknowledge that they have each had equal opportunity to negotiate the terms and conditions and participate in the drafting of this Agreement. Accordingly, this Agreement shall not be construed against any one party as the drafter but shall be construed according to its terms equally as to each party. Any rule of construction against the drafter is hereby waived by each of the parties as to this Agreement.

WITS Master License Agreement

16. Disputes.

- 16.1. Except for any suit seeking injunctive relief to enforce the proprietary rights or protect the confidential information of either party, the parties will attempt in good faith to resolve promptly through negotiation any claim or controversy arising out of or relating to this Agreement. If a claim or controversy should arise, representatives of the parties shall meet at least once and will attempt in good faith to resolve the dispute. For such purpose, either party may request the other to meet within fifteen (15) days at a mutually agreed upon time and place. If the parties are not able to conduct a meeting within the fifteen (15) day period or to resolve the dispute within thirty (30) days after their first negotiating meeting (or such longer period of time as may be mutually agreed upon), either party may refer the claim or controversy to non-binding mediation by sending a written mediation request to the other party. In the event that such a request is made, the parties agree to participate in the mediation process. The parties further agree that their participation in mediation is a condition precedent to any party pursuing any other available remedy in relation to the dispute.
- 16.2. The parties must jointly appoint a mutually acceptable mediator. If the parties are unable to agree upon the appointment of a mediator within seven (7) days after a party has given notice of a desire to mediate the dispute, any party may apply to the American Arbitration Association, or such other organization or person agreed to by the parties in writing, for appointment of a mediator.
- 16.3. The parties and the mediator may join in the mediation any other party necessary for a mutually acceptable resolution of the dispute. Should the mediator at any time be unable or unwilling to serve, the parties shall select a successor mediator. The mediation procedure shall be determined by the mediator in consultation with the parties.
- 16.4. If the dispute or claim is resolved successfully through the mediation, the resolution will be documented by a written agreement executed by all parties. If the mediation does not successfully resolve the dispute or claim, the mediator shall provide written notice to the parties reflecting the same, and the parties may then proceed to seek an alternative form of resolution of the dispute or claim, in accordance with the remaining terms of this agreement and other rights and remedies afforded to them by law.
- 16.5. The parties further acknowledge and agree that mediation proceedings are settlement negotiations, and that, to the extent allowed by applicable law, all offers, promises, conduct and statements, whether oral or written, made in the course of the mediation by any of the parties or their agents shall be confidential and inadmissible in any arbitration or other legal proceeding involving the



WITS Master License Agreement

parties; provided, however, that evidence which is otherwise admissible or discoverable shall not be rendered inadmissible or non-discoverable as a result of its use in the mediation.

- 16.6. The parties further agree to share equally the costs of the mediation; such costs will not include costs incurred by a party for representation by counsel at the mediation.

17. Excusable Delay.

- 17.1. In no event shall either party be liable one to the other for any delay or failure to perform hereunder, the delay or failure to perform due to causes beyond the control of said party, including, but not limited to, acts of God, acts of the public enemy, terrorism, civil disturbance, acts of any government, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes, and unusually severe weather conditions.

18. Notices.

- 18.1. All notices, orders, directives, requests, or other written communications required or permitted to be given or sent pursuant to this Agreement shall be deemed given (or issued) if sent by overnight courier or first-class mail addressed as follows:

In the case of Licensor to:

FEI.COM, INC. dba FEI Systems
9755 Patuxent Woods Drive, Suite 300
Columbia, Maryland 21046

In the case of Licensee to:

Name: [INSERT COMPANY NAME]
Address: [INSERT COMPANY ADDRESS]

- 18.2. Either party may, by written notice given in accordance with the foregoing, change its address or designated recipient for notices. Any notice given as aforesaid shall be deemed to have been received on the day after the date of the overnight mail receipt or three (3) working days after deposit in the mail (first-class, postage prepaid), whichever is applicable.



WITS Master License Agreement

19. Assignment.

19.1. This Agreement is personal to Licensor and Licensee, and the rights, duties and obligations of Licensee under this Agreement may not be assigned by Licensee in whole or in part by operation of law or otherwise without the prior express written consent of Licensor, at its sole discretion, and any attempted assignment of any rights, duties or obligations hereunder without such consent shall be null and void. This Agreement shall then be binding on the parties and their permitted assigns.

20. Miscellaneous

20.1. Survival. Any provisions of this Agreement which by their nature or as drafted extend beyond its termination, including without limitation the provisions relating to the obligations of confidentiality of the parties hereunder, and any provisions which survive by action of statute, shall survive the completion, rescission, or termination of this Agreement.

20.2. Severability. In the event that any one or more of the provisions of this Agreement shall for any reason be held invalid, illegal, or unenforceable, the remaining provisions of this Agreement shall be unimpaired, and the invalid, illegal, or unenforceable provisions shall be replaced by a mutually acceptable provision, which being valid, legal, and enforceable, comes closest to the intention of the parties underlying the invalid, illegal, or unenforceable provision.

20.3. Governing Law. The validity of this Agreement, the construction and enforcement of its terms, and the interpretation of the rights and duties of the parties shall be governed by the laws of the State of Maryland, without regard to its conflict of laws principles and without regard to Maryland Uniform Computer Information Transactions Act

20.4. Entire Agreement. This Agreement and any Addenda thereto represent the entire agreement between Licensor and Licensee with respect to the subject matter herein, and Licensor and Licensee agree that all other agreements, purchase orders, proposals, order forms, representations, and other understandings dated prior to this agreement, whether written or oral, concerning the Licensed Software, are superseded in their entirety by this Agreement.

20.5. Modification, Amendment, Supplement, and Waiver. No alteration, modification, attachment, supplement, or exhibit to this Agreement shall be valid unless made in writing and signed by Licensor and Licensee. A failure or delay by either party to this Agreement to enforce, at any time, any of the



WITS Master License Agreement

provisions of this Agreement, to exercise any option which is herein provided, or to require at any time performance of any of the provisions hereof shall in no way be construed to be a waiver of any provision of this Agreement.

21. Headings.

- 21.1. The headings of this Agreement are for reference purposes only and shall not in any way limit or affect the meaning or interpretation of any of the terms.

**REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK.
SIGNATURE PAGE TO FOLLOW.**



WITS Master License Agreement

LICENSOR AND LICENSEE, HAVING READ AND UNDERSTOOD THIS AGREEMENT AND ANY EXHIBITS, ATTACHMENTS, AND ADDENDA CONSTITUTING A PART HEREOF, AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS LICENSE.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and the year first above written.

LICENSOR:
FEI.COM, INC.

WITNESS: _____

BY: Rodney Conrad

TITLE: Deputy COO, GM-FEI Products

DATE: _____

LICENSEE:

WITNESS: _____

BY: _____

TITLE: _____

DATE: _____

WITS Developed Modules
Schedule A
(Last Updated August 25, 2020)

The modules listed below serves as a list of modules developed by the WITS collaborative. There is no implication that any of these modules can be deployed in a production version of WITS at no cost.

Administration

- Agency Events
- Agency Management
- Facility Management
- Facility/Staff Licensure
- Program Management
- Staff Management
- Support Ticket

Clinical / Case Management

- Admission
- Agency Waitlist Management
- Alerts
- Bed Management
- Case Management
- Consolidated Clinical Document Architecture (CCDA)
- Client Dashboard
- Client Profile
- Clinical Dashboard
- Consent and Referral
- Court Modules and Re-Entry
- Crisis Screening and Contact Management
- Crisis workflow
- Diagnosis
- Discharge
- Discharge Planning
- Dispensary Management
- Document Management
- Drug Testing and Results
- E-Prescribing
- Group Notes
- Health Information Management
- Immunizations
- Inpatient Unit Management
- Inpatient/Residential Bed Management
- Intake
- Licensed Practitioner of the Healing Arts (LPHA) Dashboard
- Manual Lab Orders

- Outcome Measures
- Prevention Planning and Implementation
- Program Enrollment/Disenrollment
- Provider Accreditation Module
- Recovery Planning and Review
- Scheduler
- Treatment Encounters
- Treatment Planning and Review
- Treatment Teams
- Vitals

Grant Management

- Government Performance and Results Act (GPRA)
- Grant Management Dashboard
- Screening, Brief Intervention and Referral to Treatment (SBIRT) Workflow
- Access to Recovery (ATR) Workflow and Voucher Management

Assessments / Screeners*

- Numerous assessments/screeners (contact FEI Account Manager for a comprehensive list)

*Some screeners/assessments may require approval by a third-party copyright holder and may have a fee arrangement with the copyright holder.

Reporting

- Reports Inventory
- Excel / PDF Reports Based on Clinical/Case Management modules
- TEDS/NOMS/URS Data Reporting

Billing

- 3rd Party Billing (837p/837i; 999; 835)
- Contract Management and Payor Adjudication
- Authorization Management
- Provider and Client Invoicing