Privacy Impact Assessment for the VA IT System called:

Westat FISMA High Enclave (FHE)

Veterans' Health Administration (VHA)

Office of Research and Development

eMASS ID# 1063

Date PIA submitted for review:

01/09/24

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Michelle Christiano	Michelle.Christiano@va.gov	(706) 339-7980
Information System Security Officer (ISSO)	Stuart Chase	Stuart.Chase@va.gov	(410) 340-2018
Information System Owner	Joseph Holston	Joseph.Holston@va.gov	(202) 443-5622 (202) 746-7872

Abstract

The abstract provides the simplest explanation for "what does the system do?".

The Westat FISMA High Enclave (FHE) is an information system enclave operated by Westat to support research and other activities conducted by Westat for the Veterans' Health Administration. It consists of a network enclave (i.e., an isolated network segment), a secure workspace, a secure equipment rack, secure media/materials storage, data network cables and equipment, servers, workstations, and peripheral devices.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

System Name: Westat FISMA High Enclave (FHE) Program Office: Office of Research Development

B. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

Westat's FISMA High Enclave (FHE) is a secure host environment operated by Westat to support research and other activities conducted by Westat for the Veterans Administration. It consists of a network enclave (i.e., an isolated network segment), a secure workspace, a secure equipment rack, secure media/materials storage, data network cables and equipment, servers, workstations, and peripheral devices. The FHE is a complete and secure computing environment, with an efficient office-style workroom, secure media and file storage, several individual workstations, a printer, and office equipment and supplies. Workrooms are secured by cipher locks. Media storage containers are secured using key or combination locks. System network resources include web servers, a file server, database servers, and utility servers for system monitoring and backups. The FHE's computing platform is designed to support the development and implementation of web applications to support data collection via web, paper, and telephone surveys; perform data analysis and reporting and delivery of data to VA research projects under contract with Westat. Information collected and processed by these data collection systems is stored and managed within the FHE system boundary.

C. Who is the owner or control of the IT system or project?
The Westat FHE is owned and operated by Westat but controlled by the VA.

2. Information Collection and Sharing

D. What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?

The types, sizes, and sensitivity of the information utilized by VA projects vary according to specific VA research studies/projects. Some projects may store no privacy-related information at all. However, the FHE is set up for and has supported VA research, gathering information from many thousands of Veterans, as directed, and contractually required by VA. The expected number of individuals whose information is collected managed and stored within the FHE varies by VA contract. Data managed and collected for an individual VA contract can be as few as 1,000 to as many several thousand depending on the nature of the research study. The authority for the system is Title 38, United States Code, chapter 73, section 7301.

E. What is a general description of the information in the IT system and the purpose for collecting this information?

The purpose of collecting this information is to support the research, analysis, and reporting objectives of a VA contract.

F. What information sharing is conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.

Information sharing may occur with external partner organizations that work with Westat as part of the VA contract or with vendors that provide support for specific services. For example, a file containing the names and addresses of Veterans may be shared with a print vendor responsible for mailing hardcopy questionnaires to study participants.

G. Is the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?

The FISMA High Enclave (FHE) is operated in one site location, on Westat's corporate campus located at 1600 Research Blvd, Rockville, MD 20850.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

34VA10 "Veteran, Patient, Employee, and Volunteer Research and Development Project Records—VA" Published in the Federal Register / Vol. 86, No. 118 / Wednesday, June 23, 2021 / Notices indicated as "AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Section 7301. ", https://www.govinfo.gov/content/pkg/FR-2021-06-23/pdf/2021-13141.pdf

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The system is not in the process of being modified.

4. System Changes

J. *Will the completion of this PIA will result in circumstances that require changes to business processes?*

No – completion of this PIA will not result in circumstances that require changes to any business processes.

K. *Will the completion of this PIA could potentially result in technology changes?*

No- completion of this PIA will not result in any technology changes.

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone

Number, etc. of a different individual)
☒ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☒ Medical Record Number
☒ Gender
☐ Integrated Control Number (ICN)
☒ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements: Current occupation, Level of Education, Income or Medical related may be collected as part of a survey to support a VA research project.

PII Mapping of Components (Servers/Database)

Westat's FISMA High Enclave (FHE) consists of **six** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **FHE** and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Database Server	Yes	Yes	Web survey response data (survey response varies by VA contract/project) Sample of study participants –	Support the collection and administration of web, paper, and telephone surveys	Restricted user access to database server; User, Application, and Network access restrictions and security.

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

			Name, address, city, state, zip, email address, survey PIN		Role-based access to databases and database servers. Firewall segments from the public internet
SFTP Server	Yes	Yes	Sample file(s) from the VA contains: Name, address, city, state, zip, email address, survey, Marital status, health care provider information health care benefits information, VA services received; education; data of birth /death; race/ethnicity; SSN; Other PII/PHI	Supports data file exchanges with VA and Partner organizations	Requires User account approval, and user authentication. Automatic removal of data files (24hrs)
Windows File Share Server	No	Yes	Project artifacts: Analytic data files Word Documents, PDF files, Excel files, SAS datasets, other project-specific documents	Project file share. Supports daily work activities conducted by project staff	Requires 2-factor authentication Restricted user access to file share; data encryption. behind firewall
Teleform Image Capture Server	Yes	Yes	Paper survey response data (survey data varies by VA contract)	Supports mail survey data collection and processing	Requires 2-factor authentication Restricted user access to Teleform Server

Alchemy Repository Server	No	Yes	Stores scanned images of hardcopy mail survey returns	Stores scanned images of hardcopy mail survey returns	Requires 2-factor authentication Restricted user access to image repository, data encryption, behind firewall

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Privacy-related information is typically provided by the contracted VA organization, collected directly from the individual, acquired from other government agencies (e.g., SSA), or retrieved from non-federal or commercial aggregator services such as Lexis-Nexis, Anchor Computing, or White pages for example.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

Information from other sources is used to support the research requirements and objectives of the individual VA contract. Additional data is used to augment study information and update participant information such as addresses and phone numbers, to ensure that study information is current and study participants are not inadvertently contacted. To support hardcopy mailing and tracing of individuals, Westat could use one or more of the following commercial services to perform individual tracing to update contact information for a Veteran. They include:

- White pages Premium (https://www.whitepages.com)
- Fast people (https://www.fastpeoplesearch.com)
- General Google search
- Property searches
- True people (https://www.truepeoplesearch.com
- Obituaries
- US Phone Book
- People Finders (https://www.peoplefinders.com/)
- Voter Registration

- USA People Search (https://www.usa-people-search.com/address-search)
- LinkedIn (through Google search)
- National Change of Address (NCOA)

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

Systems that collect data on behalf of a VA research project under contract with Westat may have as part of its study requirements, data analysis and reporting. As part of the data analysis derived variables, scores, and weighting variables may be created as part of these tasks. Additionally, statistical reports containing these derived variables may be created and used as part of the VA contract to report the outcomes of the research study.

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Information is collected in a variety of ways, depending on the requirements of the contracting VA organization. These include:

- Paper forms, typically surveys completed by individual respondents or participants.
- Web surveys and online forms completed by study participants or completed by a telephone interviewer by phone.
- Data files provided by the contracting VA organization.
- Data files provided by other agencies or organizations, which are provided through the contracting VA organization and stored as electronic data files within the FHE.
- WebEx teleconferencing software to support cognitive interviews and focus groups with a small group of study participants to test how well study participants understand survey questions and other survey materials.
- Data generated by project staff (e.g., receipt control data, data collected via telephone, scans, etc.) and stored as electronic files or data within the FHE.

- Westat also may use vendor lookup services to perform individual tracing to update contact information and phone numbers of select study participants who have incomplete or inaccurate contact information. VA data is not shared directly with these vendor services. The following is a list of vendors Westat may use to perform this task.
    - White pages Premium (https://www.whitepages.com)
    - Fast people (https://www.fastpeoplesearch.com)
    - General Google search
    - Property searches
    - True people (https://www.truepeoplesearch.com

- Obituaries
- US Phone Book
- People Finders (https://www.peoplefinders.com/)
- Voter Registration
- USA People Search (https://www.usa-people-search.com/address-search)
- LinkedIn (through Google search)
- National Change of Address (NCOA)

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

OMB control number will vary by VA contract. The current OMB control number for the 2023 VA Survey of Enrollees is 2900-0609

1.4 How will the information be checked for accuracy? How often will it be checked?

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Information is checked for accuracy by methods consistent with best practices for the contracted activity. These methods may include, but are not limited to, cross-check comparisons between sources, statistical analysis, data validation, and periodic review.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

Westat uses Statistical Analysis System (SAS) to verify information and SQL queries to check the accuracy of information in data files provided or collected as part of a research study. Methods may include, but are not limited to, cross-check comparisons between sources, statistical analysis, data validation, and periodic review.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

Privacy-related information is collected under legal authorities cited or referenced in the individual project contracts. The FHE supports VA projects at Westat, as directed and authorized by the contracting VA organization. The authority for the system is Title 38, United States Code, chapter 73, section 7301.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk:
Disclosure of a body of personally identifiable information, which may include SSNs, that if disclosed may expose the individual to financial loss or identity theft. Disclosure of military service details that may compromise the individual's reputation, circumstances, or safety. Disclosure of medical, personal, or other information that may compromise the individual's reputation or circumstances. Disclosure of participation in a particular study or activity, where knowledge of participation may adversely impact the individual's reputation or circumstances.

Mitigation:
The information system is protected through adherence to the NIST Risk Management Framework, for data at the High sensitivity level. This includes the implementation of all required security controls as described in NIST Special Publication 800-53 Revision 5, "Security and Privacy Controls for Federal Information Systems and Organizations".

Information is secured by the FHE through the use of access controls, personnel security awareness and training, regular auditing of information, and information management processes. Additionally, careful monitoring of a properly authorized information system, control of changes

to the system, appropriate handling and testing of contingencies and contingency planning, ensuring that all users of the information system are properly identified and authorized for access and that they are aware of the rules and acknowledge that fact, by ensuring that any incident is handled expeditiously. Properly maintaining the system and regulating the environment the system operates in, controlling media, evaluating risks and planning for information management and information system operations, by ensuring that the system and any exchange of information is protected, by maintaining the integrity of the system and the information stored in it, and by adhering to the requirements established in applicable contracts.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system that will be used in support of the program's business purpose.

All information managed in the FHE is used to support research studies under contract between Westat and the Veterans Administration. Data and information are used to conduct web, paper, and phone surveys, statistical/data analysis, and reporting for the Veterans' Administration. Privacy-related information is typically used for:

- Contacting prospective participants
- Requesting information from other sources (if required)
- Statistical processing and analysis
- Longitudinal data collection/generation
- Aggregation into de-identified (i.e., abstracted or aggregated) data products
- Aggregation into de-identified reports and publications

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

PII/PHI Data Element	Internal Use	External Use
Name of Veteran	Used as study participant identifier	Used to send hard copy mailing materials
Social Security Number (SSN)	Used as study participant identifier	Only of if necessary to obtain administrative records or other information to support the study
Date of Birth	Used to identify participants' age and confirm participants' identity	Not used externally --but may be included in a survey results file delivered to VA
Mailing Address	Used to send hard copy mailing materials	Used to send hard copy mailing materials

Email Address	Used to send email notifications and follow-up reminders to study participants.	Not used externally - but may be included in a survey results file delivered to VA
Financial Information	Information such as annual income may be collected as part of a survey in support of a VA research study	Not used externally--but may be included in a survey results file delivered to VA
Internet Protocol	Collected as part of the web survey application, captured in server logs	Not used externally
Medications	May be collected as part of a web or mail survey	Not used externally - but may be included in a survey results file delivered to VA
Medical Record number	Unique identifier to look up medical history as part of a VA research study	May be shared with the VA to obtain related information or included in a survey results file delivered to VA
Race Ethnicity	May be collected as part of a survey and used to support data analysis	Not used externally - but may be included in a survey results file delivered to VA
Gender	Maybe collected as part of a survey and used to support data analysis	Not used externally - but may be included in a survey results file delivered to VA
Military History/Service	Maybe collected as part of a survey and used to support data analysis by military branch/service	Not used externally - but may be included in a survey results file delivered to VA
Survey Username, Password, or PIN	Used to authenticate a survey respondent	Not used externally
Sample ID	Uniquely identify a survey participant and link survey response data to the respondent	Not used externally may be included in a data file delivered to the VA

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

Research projects supported by the FHE may perform a variety of analyses of privacy-related data. At Westat, this is usually performed using Statistical Analysis System (SAS.) and

Excel. New information about individuals may be generated as inputs to analysis or as intermediate products during analysis. Privacy-related data are most often not included in the final, deliverable research results.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

Research projects supported by the FHE may perform a variety of analyses of privacy-related data. At Westat, this is usually performed using Excel and Statistical Analysis System (SAS.) New information about individuals may be generated as inputs to analysis or as intermediate products during analysis. Privacy-related data are most often not included in the final, deliverable research results. Any action taken for or against an individual because of any derived data /information or that is made available to the government, or its employees is done at the discretion of the VA, not by Westat.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

The information system is protected through adherence to the NIST Risk Management Framework, for data at the High sensitivity level. This includes the implementation of all required security controls as described in NIST Special Publication 800-53 Revision 5, "Security and Privacy Controls for Federal Information Systems and Organizations". Confidential or sensitive information is protected during transmission to and from Westat computer systems using Transport Layer Security (TLS), digital certificates, and signatures that encrypt data, validate data integrity, and authenticate the parties in a transaction. Electronic data files are stored on a project-specific network folder on the FHE network and only designated project staff have access to this folder. Microsoft Active Directory controls user access. All users are required to authenticate using two-factor authentication to login to workstations. Workstations are in secured rooms and all servers are in a locked cabinet inside Westat's secure Data Center.

Hardcopy material or system-generated output containing confidential data is stored in secure rooms and locked cabinets. Westat's FHE network consists of a system of redundant firewalls and redundant Internet connections to support websites, email, and SFTP access for projects and corporate functions requiring these services. Several network zones with varying levels of access restrictions have been established on the firewall. With this configuration, resources that require restricted access controls, such as database servers that manage and store PII, can be kept separate from resources that need to be more generally accessible, such as web surveys, websites or other web applications hosted on public-facing web servers. Intrusion detection software running on our firewalls detects and blocks outside users who are identified as attempting to gain unauthorized access to our network.

Intrusion detection signature patterns are automatically updated regularly by the firewall application vendor to keep pace with the latest techniques used to break into networks. Westat performs vulnerability scans weekly on servers to identify possible vulnerabilities. Results are made available to the appropriate systems technical administrators and managers who are required to respond with information on any corrective actions taken. Server and workstation operating systems are updated with applicable security patches as they are made available by the vendor.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

See the response above. In addition, Westat takes additional steps to protect electronic data files that contain SSNs. Electronic data files containing SSN are encrypted using FIPS 140-2 certified encryption software and the file is password protected using a strong password comprised of alpha-numeric and special characters with a length of at least 8 characters. The encrypted data file is also stored in a project-specific network folder within FHE, and only designated project staff have access to this folder. Access is controlled by Microsoft Active Directory. SSN is never used as a primary key in any database or displayed in any information system (especially public facing) used to support VA research study at Westat. If necessary Westat will create a random ID that can be used to link to the electronic file containing SSN to conduct any subsequent data retrieval or data analysis on a study participant record.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

Westat in collaboration with the VA information security team conducts a security control assessment annually on all administrative, technical, and physical controls to ensure that all sensitive and confidential data are properly managed, stored, and protected at all times. Westat performs vulnerability scans weekly on servers to identify possible vulnerabilities. Results are made available to the appropriate systems technical administrators and managers who are required to respond with information on any corrective actions taken. Server and workstation operating systems are updated with applicable security patches as they are made available by the vendor. All Westat personnel working on projects are instructed in Westat's data security policies, standards, and procedures and the importance of protecting data confidentiality. In addition, all Westat personnel are required to read and sign Westat's "Employee or Contractor's Assurance of Confidentiality of Survey Data." And are required to complete Westat and VA security awareness training annually.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

Access to PII data is determined by the Westat Sr. Project Director overseeing the VA project or FHE IT Manager and is based on a need-to-know basis.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

All access requests to FHE and project data are requested through Westat's Information Assurance (IA) SharePoint portal. All access requests are reviewed and approved by the Project Director and/or FHE IT Manager.

2.4c Does access require manager approval?

Yes – see the response above.

2.4d Is access to the PII being monitored, tracked, or recorded?

Access is tracked in the FHE Information Assurance Portal. Access to the FHE network, workstations, and data files is tracked and logged by the FHE network.

2.4e Who is responsible for assuring safeguards for the PII?

Westat's Network Operations Manager and System Administrators, Westat's Chief Information Security Officer, Westat's FHE IT Manager, Westat's Sr. Project Study Manager, Westat staff who work in the FHE and provide support to research projects.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system.*
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

Retained information may include name, race/ethnicity, SSN, date of birth, mother's maiden name, mailing address, zip code, phone number(s), email address, financial account information, medications and medical record information, survey response data, and IP addresses.

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

All VA information is retained by individual projects in accordance with the VA-NARA retention agreement. All records acquired or generated by a project are retained for the duration of the project and are the responsibility of the contracting organization thereafter. VA projects currently under contract with Westat require data to be retained for the length of the contract and destroyed immediately after the period of performance. VA projects currently under contract with Westat require data to be retained for 3 years and destroyed after the period of performance. Under no circumstances is VA information retained in the FHE beyond the expiration of the contract authorizing the utilization of that information.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Retention schedules for the information systems hosted by Westat in the Westat FHE are determined by the individual contracts established between the VA and Westat to support specific data collection, research, and analysis studies. Current VA contracts supported by Westat required data to be retained for 3 years and destroyed after the contract period of performance. The information is retained following the policies and schedules of VA's Records Management Service and NARA in "Department of Veterans Affairs Records Control Schedule 10-1". Record Control Schedule 10-1 can be found at the following link: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf.

3.3b Please indicate each records retention schedule, series, and disposition authority?

The information is retained following the policies and schedules of VA's Records management Service and NARA in "Department of Veterans Affairs Records Control Schedule 10-1". Record Control Schedule 10-1 can be found at the following link: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf.

Federal Register indicated "POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are scheduled in accordance with RCS 10–1, 8300.6, temporary disposition; cutoff at the end of the fiscal year after completion of the research project. Destroy six (6) years after cutoff. May retain longer if required by other Federal regulations or the European General Data Protection regulations. (DAA–0015–2015–0004, item 0032)".

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

Sensitive information is disposed of at Westat in accordance with VA policy and/or as directed by the contracting VA organization. Mechanisms available include shredding for paper and other materials, secure erasure for digital storage media, degaussing for magnetic media, and physical destruction for anything not securable by other means.

More specifically, media containing sensitive information are sanitized by secure erasure, low-level formatting, degaussing, irreversible disassembly, or shredding. Hardcopy media containing sensitive information are shredded and recycled. Secure bulk shredding services are provided to projects, with secure shredding bins available for hardcopy materials in Westat facilities.

Other digital media are stored in a padlocked container then degaussed and destroyed in bulk, in the same manner as backup tapes except that no transmittal letter is prepared. Media not containing sensitive information are disposed of conventionally. Media containing sensitive information are cleared, purged, or destroyed when no longer needed. Virtual systems containing sensitive information are cleared using a multi-overwrite process. All methods described conform to the NIST Special Publication 800-88, "Guidelines for Media Sanitization".

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what

controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

Westat does not use actual PII for research, testing, or training. Dummy data is used for research, testing, or training purposes.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk:
Disclosure of a body of personally identifiable information, which may include SSNs, that if disclosed may expose the individual to financial loss or identity theft. Disclosure of military service details that may compromise the individual's reputation, circumstances, or safety. Disclosure of medical, personal, or other information that may compromise the individual's reputation or circumstances. Disclosure of participation in a particular study or activity, where knowledge of participation may adversely impact the individual's reputation or circumstances.

Mitigation:
Information is secured on the system through access controls, personnel security awareness and training, regular auditing of information, and information management processes. Additionally, careful monitoring of a properly authorized information system, control of changes to the system, appropriate handling, and testing of contingencies and contingency planning, ensuring that all users of the information system are properly identified and authorized for access and that they are aware of the rules and acknowledge that fact, by ensuring that any incident is handled

expeditiously. Properly maintaining the system and regulating the environment the system operates in, controlling media, evaluating risks, and planning for information management and information system operations, by ensuring that the system and any exchange of information are protected, by maintaining the integrity of the system and the information stored in it, and by adhering to the requirements established in applicable contracts.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
N/A	N/A	N/A	N/A

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document in this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System	***List the purpose of information***	***List the specific PII/PHI data elements that are***	***List the legal authorit***	***List the method of transmission and***

information is shared/received with	***being shared / received / transmitted with the specified program office or IT system***	***processed (shared/received/transmitted)with the Program or IT system***	***y, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***the measures in place to secure data***
Trilogy (Small Business Partner)	Obtain sample file information for research study	Name, address, city, state, zip, email address, survey PIN, Marital status, health care provider information health care benefits information, VA services received; education; data of birth /death; race/ethnicity; SSN; Other PII/PHI	MOU	Secure FTP
LexisNexis (Locating Veterans)	To obtain current address and phone numbers of study participant	Name, last known address, last known phone number, SSN	MOU	Secure FTP
Anchor Computing https://anchorcomputer.com solutions/data-quality/	To obtain current address and phone numbers of study participant	Name, last known address, last known phone number, SSN	MOU	Secure FTP
VHA (Westat FHE operates under a VA ATO)	Obtain sample file information	Per VHA, data elements shared could be survey results collected,	Varies by contract. BAA/	Secure FTP

	for research study. Provide survey research results at the end of the study	PHI and PII, sample file information and/or other administrative data used to support the administration of the survey	MOA / LOI when needed	
Navistar (Primary Print Vendor) https://www.navistardirect.com	To support the printing and mailing of hardcopy surveys to study participants	Name, address, city, state, zip –	MOU	Secure FTP
NPC (backup Print Vendor if needed) https://www.npcweb.com	To support the printing and mailing of hardcopy surveys to study participants	Name, address, city, state, zip –	MOU	Secure FTP
National Change of Address (NCOA)	Service used to obtain updated address information to support hardcopy survey mailings	Name, address, city, state, zip –	MOU	Secure FTP

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk:

Inadvertent disclosure of information contained in data files exchanged with external agencies or partner organizations if disclosed may expose the study participant to financial loss, or identity theft or could harm the reputation of the study participant or the VA organization.

Mitigation:

Information-sharing agreements such as MOU, BAA, and MOA are established with outside agencies and/or partner organizations which stipulate how information should be used and managed in support of the research conducted as part of the VA contract.

Access controls are in place to ensure that only authorized staff have access to the information systems and services provisioned by the Westat FHE. Data files exchanged with external organizations in support of the contract only contain data elements necessary to perform the services as specified in the contract, agreement, or task order with that organization. For example, only name and mailing address are provided to the external print vendor supporting hard copy survey mailings. Data files exchanged with external organizations are done using the SFTP site provisioned by the Westat FHE. All users are required to have a valid user id and password and must be approved by the Project Director before they are granted permission to access the SFTP site. All user logins file uploads, and download activities are tracked in SFTP server logs.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the

Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Individuals are notified prior to data collection in accordance with VA policy and direction by the contracting VA organization. Notification varies based on the type of research study. An example of the pre-notification is attached for reference (Appendix A-6.1).

34VA10 "Veteran, Patient, Employee, and Volunteer Research and Development Project Records—VA" Published in the Federal Register / Vol. 86, No. 118 / Wednesday, June 23, 2021 / Notices indicated as "AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Section 7301. ", https://www.govinfo.gov/content/pkg/FR-2021-06-23/pdf/2021-13141.pdf.

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

All notices provided to study participants are reviewed and approved by the Westat Project Director and the VA COR to ensure all information provided is adequate to inform those affected by the research study and that ensure them that their information is collected, managed, and used appropriately and follow VA policy directives.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

All notices provided to study participants are reviewed and approved by the Westat Project Director and the VA COR to ensure all information provided is adequate to inform those affected by the research study and that their information is collected, managed, and used appropriately and follows VA policy directives.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Research activities conducted by Westat for VA that collect information from individuals are typically surveys in which participation by the individual is voluntary. No penalties attach to refusal to participate, though incentives sometimes provided to encourage participation are not typically given to those who choose not to do so.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent

is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

Research activities conducted by Westat for VA that collect information from individuals are typically surveys in which analysis and reporting are the only uses. That is, participation is consenting to the sole intended use.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk:
The privacy risk is if Westat does not adequately inform study participants of the privacy risks to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII).

Mitigation:
Privacy, data use, and confidentiality statements as well as consent forms are provided with all data collection materials and as required, posted on information systems that collect data related to a study participant selected for a research study in accordance with VA policy and direction.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web***

page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

Activities conducted under a VA contract at Westat are typically posted to a website with contact information. Those that distribute paper forms include explanatory and contact information with the forms. Those that employ web-based data collection mechanisms send paper materials and also include contact information, usually including email addresses, and privacy notices on the website in accordance with VA policy and direction. https://vhasoe.org/#FAQ.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

The system is not exempt from the access provisions of the Privacy Act

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

The system is a Privacy Act System

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals contact the project email address or call a 1-800 number provided on the website or in survey materials.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are notified of these procedures in the survey materials, website, or privacy notice as required by the contracting organization. See Appendix A-6.1

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and

Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

In addition to contacting project staff, survey respondents often have the option of supplementing, editing, or deleting their contact information and survey responses.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk:

There is a risk that incorrect information could be stored on FHE because that information was incorrectly updated in the source systems or data sources (files/databases) provided by that source system.

Mitigation:

Subjects have previously consented to having their data stored on the systems that provide the information that is stored on FHE through the HIPAA authorization and subject consent process. If a subject's information in incorrect, the subject will need to access, redress, and correct that information via the source systems' access, redress, and correction processes. Veterans selected to participate in a particular research study are provided with a toll-free number, that they can use to find out about more details related to the study and can also request to make corrections to any contact information or request to be removed from the research study being conducted. Privacy and data use and confidentiality statements are also provided with all data collection

materials as well as posted on any information systems that collect data related to a study participant selected for a research study.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

Individuals may access information only after passing VA background screening and authorization by an identified approval authority (e.g., the VA project officer or the Westat project director). Individuals and associated access privileges are tracked in a roster. All staff are required to sign Non-Disclosure Agreement, Confidentiality Agreements Rules of Behavior, have background screenings and take VA security awareness and privacy training as required by the VA. Contracts are reviewed monthly by the COR and annually by VA finance representatives.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

No users from other government agencies outside the VA have access to the system.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Westat staff have access to information based on the roles assigned to them and as authorized by the VA project officer(s) or Westat project director(s) of the project(s) to which each individual is assigned. Roles include Web/Database developers, SAS analysts, Network Admins, Project support staff, and Field Room staff.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access

to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Per the VA contract, Contractors are only allowed to access the SFTP site provisioned by the FHE to exchange encrypted data files for a given project. All contractors are required to sign a MOU, BAA, or NDA as required by the VA contract.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.
Westat employees are required to take Westat HIPAA training, Security Awareness Training and VA security training provided in the VA TMS. All Westat staff are required to sign the FHE Rules of Behavior.

8.4 Has Authorization and Accreditation (A&A) been completed for the system? Yes

8.4a If Yes, provide:

1. *The Security Plan Status:* ***Approved***
2. *The System Security Plan Status Date:* ***June 26, 2023***
3. *The Authorization Status:* ***Approved***
4. *The Authorization Date:* ***Aug 11,2023***
5. *The Authorization Termination Date:* ***July 27, 2025***
6. *The Risk Review Completion Date:* ***Aug 4, 2023***
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* ***HIGH***

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***
N/A

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

The FHE does not use cloud technology.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

The FHE does not use a Cloud Service Provide (CSP).

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

The FHE does not use a CSP.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

The FHE does not use a CSP.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

The FHE does not utilize Robotic Process Automation (RPA).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice

ID	Privacy Controls
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

MICHELLE CHRISTIANO

Digitally signed by MICHELLE CHRISTIANO
Date: 2024.02.13 11:57:23 -05'00'

Privacy Officer, Michelle Christiano

STUART CHASE

Digitally signed by STUART CHASE
Date: 2024.02.13 12:04:10 -05'00'

Information Systems Security Officer, Stuart Chase

JOSEPH HOLSTON

Digitally signed by JOSEPH HOLSTON
Date: 2024.02.27 17:05:13 -05'00'

Information Systems Owner, Joseph Holston

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

https://vhasoe.org/#FAQ

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices