Privacy Impact Assessment for the VA IT System called:

Westat FISMA High Enclave (FHE)
VACO
National Services

Date PIA submitted for review:
October 5th, 2022

System Contacts:

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Kimberly E. Murphy</td>
<td><a href="mailto:Kimberly.Murphy@va.gov">Kimberly.Murphy@va.gov</a></td>
<td>(781) 331-3206</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Stuart Chase</td>
<td><a href="mailto:Stuart.Chase@va.gov">Stuart.Chase@va.gov</a></td>
<td>(410) 340-2018</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Joseph Holston</td>
<td><a href="mailto:Joseph.Holston@va.gov">Joseph.Holston@va.gov</a></td>
<td>(202) 443-5622 (202) 746-7872</td>
</tr>
</tbody>
</table>
Abstract

The abstract provides the simplest explanation for “what does the system do?” and will be published online to accompany the PIA link.

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’ 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:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- Indicate the ownership or control of the IT system or project.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- A general description of the information in the IT system and the purpose for collecting this information.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether 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.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes
- Whether the completion of this PIA could potentially result in technology changes
- 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 FISMA High Enclave (FHE) is operated in one location, at Westat’s corporate campus in Rockville, MD. It provides scientific and technical support to program evaluations, research, analysis, and the management and operations of VA projects that have stringent security requirements.
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 supports various VA research studies that require systems/applications to collect data via web, paper and telephone surveys; data analysis and reporting and delivery of data to the VA to support the research objectives of the study. Surveys support the research objectives specified in the project contracts.

Web-based surveys are self-administered. Paper, and telephone surveys are conducted by Westat project staff members. Information collected by these surveys is stored and managed in the FHE. The FHE’s computing platform is designed to host and support the development and implementation of websites, web based survey applications and client-server applications.

Applications are developed using Microsoft’s .NET framework. Data are stored in Structured Query Language (SQL) databases using Microsoft’s SQL Server RDMS. The Westat FHE also supports the development and execution of statistical analysis scripts in SAST™ and SPSS to support data analysis and reporting; Cardiff Teleform to support scanning and verification of paper surveys and Microsoft Office software for ad-hoc reporting and analysis.

The information in the system may include privacy-related information such as personally identifiable information (PII) as defined by the Privacy Act of 1974, information in identifiable form (IIF) as defined by the E-Government Act of 2002, and protected health information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA), as well as other forms of sensitive information such as statistical data protected under the Confidential Information Protection and Statistical Efficiency Act (CIPSEA), information protected by the Policy for the Protection of Human Subjects (e.g., the “common rule”), controlled unclassified information (CUI), and information exempted from release under the Freedom of Information Act (FOIA).

The types, size, and sensitivity of the information utilized by VA projects varies according to specific VA research study/project. Some projects may store no privacy-related information at all. However, the FHE is setup 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

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.

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 Account Information
- Health Insurance Beneficiary Numbers Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications Address Numbers
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Gender
- Integration Control Number (ICN)
- Military History/Service Connection
- Next of Kin
- Other Unique Identifying Information (list below)

Survey respondent unique identifying code and details of military service may also be collected.

**PII Mapping of Components**

The Westat FHE does not consists of any key components as there are no internal database connections with VA.
PII Mapped to Components

Database Name of the information system collecting/storing PII | 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
--- | --- | --- | --- | --- | ---
N/A | N/A | N/A | N/A | N/A | N/A

1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Privacy-related information is typically provided by the contracted VA organization, collected from the individual, acquired from other government agencies (e.g., SSA, IRS), or retrieved from non-federal or private organizations.

The information is provided by the contracted VA organization and is used to contact prospective research subjects and to correlate with information acquired from other sources. Information provided may include financial data, birth and death dates, benefits received or applied for, and other personal contact information (e.g., phone, address, email). The system is used by hosted projects to create reports, and analytic data/files as required by specific VA contracts.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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
- Online forms, also typically web surveys completed by respondents or participants or by completed by telephone interviewer by phone
- Data files provided by the contracting VA organization
- Data files provided by other agencies and organizations which are provided through the contracting VA organization and stored as electronic data files within the FHE.
- 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.

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

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.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

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 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.

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:** Information will be secured on the system through access controls, personnel security awareness and training, regular auditing of information and information management processes, 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 will be used in support of the program’s business purpose.

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.

All information in the FHE supports research and other activities conducted by Westat for the Veterans’ Administration. Privacy-related information is typically used for:

- Contacting prospective participants
- Requesting information from other sources
- 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

- SSN: Used as a patient identifier
- Phone Number: Used to contact the individual
- DoB: Used to identify patient age and confirm patient identity

- Personal mailing address: used to send hard copy mailing materials
- Personal email address: used to send email notifications and followup reminders to study participants
- Financial Account Information: information such as annual income may be collected as part of a survey in support of a VA research study
- Internet Protocol (IP) Address Numbers: is collected as part of the web survey application
- Current Medications: may be collected as part of a web or mail survey to identify current medications taken by a study participant in support of a VA research study
- Previous Medical Records: may be collected as part of a study to confirm medical history
- Race/Ethnicity: may be collected as part of a survey and used to support data analysis
- Medical Record Number: unique identifier to look up medical history
- Gender: maybe collected as part of a survey and used to support data analysis
- Military History/Service Connection: used to analyze data by military branch/service
- Other Unique Identifying Information: include any system generated identifiers that can be used to uniquely identify a survey respondent or used to link survey response data back to a respondent (e.g., Survey PIN, Sample ID)
2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

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.

2.3 How is the information in the system secured?

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

- Confidential or sensitive information is protected during transmission to and from Westat computer systems by the use of 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. Access is controlled by Microsoft Active Directory.
- All users are required to authenticate using two-factor authentication to login to workstations. Workstations are located in secured rooms and all servers are in a locked cabinet inside Westat’s secure Data Center.
- Hardcopy material or system-generated output or containing confidential data are stored in secure rooms and locked cabinets.
- Westat's FHE network consists of a system of redundant firewalls and redundant Internet connections to support web sites, 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 fairly 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, web sites 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 response above. In addition, Westat takes additional steps to protect electronic data files that contain SSN. Electronic data files containing SSN are encrypted using FIPS 140-2 certified encryption software and the file is also 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 which 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 polices, 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.

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access
documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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.

Add answer here:

The privacy impact related to uses of the information is the same as that derived from the information characterization. The primary risk is, again, inadvertent disclosure, which is mitigated as described in Section 1.7 above.

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

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. Retained information types may include name, race/ethnicity, SSN, date of birth, mother’s maiden name, mailing address, zip code, phone number(s), fax number(s), email address, financial account information, medications and medical record information, 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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. This question is related to privacy control DM-2, Data Retention and Disposal.

VA projects currently under contract with Westat require data be retained for 3 years 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)? If so please indicate the name of the records retention schedule.

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. This question is related to privacy control DM-2, Data Retention and Disposal.

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. As stated above current contracts supported by Westat required data to be retained for a 3-year 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

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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 disassembling, 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 degausses 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 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. Have policies
and procedures been developed to minimize the use of PII 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.

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 will be secured on the system through access controls, personnel security awareness and training, regular auditing of information and information management processes, 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 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

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

**4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure**

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. 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

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trilogy (Small Business Partner)</td>
<td>Print hardcopy survey instruments</td>
<td>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</td>
<td>MOU</td>
<td>Secure FTP</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----------</td>
</tr>
<tr>
<td>LexisNexis (Locating Veterans)</td>
<td>Address and phone number verification and updates</td>
<td>Name, last known address, last known phone number, SSN</td>
<td>MOU</td>
<td>Secure FTP</td>
</tr>
<tr>
<td>VHA (Westat FHE operates under a VA ATO)</td>
<td>Per VHA data elements shared could be survey results collected, PHI and PII, administrative data used to support the administration of the survey</td>
<td>Varies by contract. BAA/ MOA / LOI when needed</td>
<td>Secure FTP</td>
<td></td>
</tr>
</tbody>
</table>

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.

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, 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 login and file upload and downloaded 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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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. This question is 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.

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).

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.” This SORN can be found online at 2021-13141.pdf (govinfo.gov)

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 consent to 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.

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?

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.

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).

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.

This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Activities conducted under VA contract at Westat typically post 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.

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-level individual named on the website or 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.

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 ensure data accuracy.

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.

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?

Describe the process by which an individual receives access to the system.

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

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.

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.
Westat staff have access to information as necessary by the roles assigned to them and as authorized by the VA project officer(s) or project director(s) of the project(s) to which each individual is assigned. 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. Other than Westat staff, no contractors are allowed access to the FHE. Contracts are reviewed monthly by the COR and annually by VA finance representatives.

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.

Individuals receive both Westat and VA security awareness and privacy training.

Westat employees are required to take Westat HIPPA training, Security Awareness Training and VA security training provided in the VA TMS. All Westat staff are required sign a the FHE Rules of Behavior

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

If Yes, provide:

1. The Security Plan Status,
2. The Security Plan Status Date,
3. The Authorization Status,
4. The Authorization Date,
5. The Authorization Termination Date,
6. The Risk Review Completion Date,
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

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

If No or In Process, provide your Initial Operating Capability (IOC) date.

FHE has received a full ATO August 26, 2020- Aug 26 2023. System Categorization: High

1. The Security Plan Status, Approved
2. The Security Plan Status Date, Aug 26, 2020
3. The Authorization Status, Approved
4. The Authorization Date, Aug 26, 2020
5. The Authorization Termination Date, Aug 26, 2023
6. The Risk Review Completion Date, Aug 14, 2020
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH). HIGH
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).

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.

- No – 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)

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

- Not applicable – The FHE does not use a Cloud Service Provider (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.

Not applicable – 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.

Not applicable - 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).

Not applicable
### Section 10. References

#### Summary of Privacy Controls by Family

<table>
<thead>
<tr>
<th>ID</th>
<th>Privacy Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td><strong>Authority and Purpose</strong></td>
</tr>
<tr>
<td>AP-1</td>
<td>Authority to Collect</td>
</tr>
<tr>
<td>AP-2</td>
<td>Purpose Specification</td>
</tr>
<tr>
<td>AR</td>
<td><strong>Accountability, Audit, and Risk Management</strong></td>
</tr>
<tr>
<td>AR-1</td>
<td>Governance and Privacy Program</td>
</tr>
<tr>
<td>AR-2</td>
<td>Privacy Impact and Risk Assessment</td>
</tr>
<tr>
<td>AR-3</td>
<td>Privacy Requirements for Contractors and Service Providers</td>
</tr>
<tr>
<td>AR-4</td>
<td>Privacy Monitoring and Auditing</td>
</tr>
<tr>
<td>AR-5</td>
<td>Privacy Awareness and Training</td>
</tr>
<tr>
<td>AR-7</td>
<td>Privacy-Enhanced System Design and Development</td>
</tr>
<tr>
<td>AR-8</td>
<td>Accounting of Disclosures</td>
</tr>
<tr>
<td>DI</td>
<td><strong>Data Quality and Integrity</strong></td>
</tr>
<tr>
<td>DI-1</td>
<td>Data Quality</td>
</tr>
<tr>
<td>DI-2</td>
<td>Data Integrity and Data Integrity Board</td>
</tr>
<tr>
<td>DM</td>
<td><strong>Data Minimization and Retention</strong></td>
</tr>
<tr>
<td>DM-1</td>
<td>Minimization of Personally Identifiable Information</td>
</tr>
<tr>
<td>DM-2</td>
<td>Data Retention and Disposal</td>
</tr>
<tr>
<td>DM-3</td>
<td>Minimization of PII Used in Testing, Training, and Research</td>
</tr>
<tr>
<td>IP</td>
<td><strong>Individual Participation and Redress</strong></td>
</tr>
<tr>
<td>IP-1</td>
<td>Consent</td>
</tr>
<tr>
<td>IP-2</td>
<td>Individual Access</td>
</tr>
<tr>
<td>IP-3</td>
<td>Redress</td>
</tr>
<tr>
<td>IP-4</td>
<td>Complaint Management</td>
</tr>
<tr>
<td>SE</td>
<td><strong>Security</strong></td>
</tr>
<tr>
<td>SE-1</td>
<td>Inventory of Personally Identifiable Information</td>
</tr>
<tr>
<td>SE-2</td>
<td>Privacy Incident Response</td>
</tr>
<tr>
<td>TR</td>
<td><strong>Transparency</strong></td>
</tr>
<tr>
<td>TR-1</td>
<td>Privacy Notice</td>
</tr>
<tr>
<td>TR-2</td>
<td>System of Records Notices and Privacy Act Statements</td>
</tr>
<tr>
<td>TR-3</td>
<td>Dissemination of Privacy Program Information</td>
</tr>
<tr>
<td>UL</td>
<td><strong>Use Limitation</strong></td>
</tr>
<tr>
<td>ID</td>
<td>Privacy Controls</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>UL-1</td>
<td>Internal Use</td>
</tr>
<tr>
<td>UL-2</td>
<td>Information Sharing with Third Parties</td>
</tr>
</tbody>
</table>
Signature of Responsible Officials

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

Privacy Officer, Kimberly E. Murphy

Stuart E. Chase

Information Systems Security Officer, Stuart Chase

Information Systems Owner, Joseph Holston
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).

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).

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.” This SORN can be found online at 2021-13141.pdf (govinfo.gov)