SPLASH PAGE LANGUAGE

The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements
under the Federal Information Security Management Act (FISMA).

VA HANDBOOK 6508.1: "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," July 2015, https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=810&FType=2

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Privacy Impact Assessment for the VA IT System called:

Veterans Evaluation Services

Date PIA submitted for review:

11/18/2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Simon Caines	Simon.Caines@va.gov	202-461-9468
Information System Security Officer (ISSO)	Anita Feiertag	Anita.Feiertag@va.gov	513-289-8116
Information System Owner	Jennifer Treger	Jennifer.Treger@va.gov	202-461-9497

Abstract

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

The Veterans Evaluation Services (VES) system is designed to process compensation and pension (C&P) cases for the Veterans Benefits Administration (VBA). The VES system is in-house developed system that provides scheduling and tracking of medical disability exam requests. The system's goal is to secure, track, and then submit the completed Disability Benefits Questionnaire (DBQ) results back to the Department of Veterans Affairs (VA) when the case is completed. VES Services performs medical exams of veterans who are in the process of applying for veteran benefits.

By providing a centralized data collection system, the VES system enables the VA to efficiently and effectively collect, manage and access Veteran medical disability exam data and supporting documentation. The secure transmission of Veteran data, including Personally Identifiable Information (PII) and Protected Health Information (PHI), outside the VA system to medical provider contractor and back to VA is a major component of the VES system.

The data transmissions are one-way to the Veterans Benefit Management System (VBMS) at the Philadelphia Information Technology Center (ITC). The VES Office Management System (OMS), located in Houston, TX, uses secure file transfers via the Internet using Attachmate's Federal Information Processing Standards (FIPS) 140-02 compliant Secure File Transfer Protocol (SFTP) software.

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 Veterans Evaluation Services system is owned and operated by Veterans Evaluation Service (VES). The purpose of the VES system is to retrieve, store, update, and manage case information from cases delivered to VES. Completed DBQs and exam request statuses are returned to the VA's Veterans Benefit Management System (VBMS) via secure FTP transfer (SFTP). VES stores approximately 125,000 exam requests statuses and associated DBQs at any one point in a central and disaster recovery site, with all computers and storage provided by a private cloud without use of public cloud technology, computing platforms, or any cloud provider. Through the centralized storage of Veteran data, all PII controls are executed consistently at the production and disaster recovery sites. No Veteran data is shared with a 3rd party, only information exchange between the VA and VES occurs.

The magnitude of harm if information were disclosed would affect the VA, and VES directly. No information from the VA is shared with any 3rd parties nor is it shared with contractors within VES. As a result, there is no data held by a cloud provider for VES nor none on our behalf. The information contained within a case can include PHI, PII, contact information, and historic medical records for the Veteran.

The completion of the PIA will not result in any changes to the established privacy controls nor changes to technology or business processes for VES. No SORN changes will be needed with this PIA either. VES is operating under the following examples of legal authority:

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
- ☒ 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)

<<Add Additional Information Collected But Not Listed Above Here (For Example, A Personal Phone Number That Is Used As A Business Number)>>

PII Mapping of Components

Veterans Evaluation Service consists of **one** key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Veterans Evaluation Service** and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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

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
Veterans Evaluation Services system	Yes	Yes	Name, SSN, address, contact information, and medical history (see above for detail).	Necessary information to contact the Veteran, process a DBQ, and submit the completed DBQ back	Key PII information such as SSN is masked from all but a tiny subset of employees, all employees work on a need to know basis with the least PII/PHI provided to any employee, multiple technical safeguards as data loss prevention. FIPS 140-2 compliant encryption is used to protect data at rest and in transport. An Intrusion detection/prevention system (IDS/IPS) and firewalls are used to protect the perimeter. Antivirus, blocking of thumb drives, and internal event logging prevent the theft of PII/PHI data.

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.

The VES system exclusively retrieves data from two sources-VBMS downloads and provider-supplied DBQ responses. The VBMS case, and phone-based veteran interview, establishes the DBQs which will be reviewed with the provider. Once a schedule is set, and the veteran attends the scheduled exam, the provider logs into the OMS web portal and completes the DBQs scheduled for the veteran. Once a DBQ is completed, the Quality Assurance (QA) team reviews the DBQ(s) to ensure accurate completion of the DBQ.

If there is any clarification needed within the case, it is completed by a provider at the request of a QA. The only source of information with this process is direct from VBMS downloads and from the provider who completed the DBQs.

No commercial information is gathered nor supplied to a 3rd party and no other report/analysis is performed other than the completed DBQs. In short, all informed is supplied initially by the VA, completed by providers, and then re-submitted to the VA for benefits assessments and scoring.

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.

The initial information, veteran contact information and medical history, is directly downloaded out of VBMS by our downloading team. Once the case is accepted and built within OMS, exams are scheduled accordingly. Data entry is performed by the provider for their DBQs for that specific veteran on the VES portal. While a veteran may see multiple providers for multiple conditions, only the specified DBQs assigned to that veteran are visible to the provider. The provider fills out the DBQ on the OMS portal, SSL secured in transit, and the data is stored on encrypted volumes for data at rest.

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.

The VES OMS system stores the data initially supplied by the VA via a download from VBMS exclusively. This data includes the immediate claim as well as medical history associated with the veteran. All data is used expressly to build a case for the veteran and establish all potential conditions that the veteran suffers from. The veteran speaks to a case builder within VES through Q+A regarding all potential conditions so this data is voluntarily supplied by the veteran. Only DBQ data results are stored from a provider's exam and Q+A with the veteran. All data that VES uses ultimately goes into building a complete set of exams for the veteran.

Minor amounts of metadata are maintained for reporting, security, or operational needs. Data such as IP addresses and time spent per DBQ are examples of the metadata maintained. This data is solely and Version Date: November 2nd, 2018 Page 7 of 25 exclusively used within VES and without a 3rd party to improve the provider coverage, improve timeliness, clarify common DBQ questions, address billing accuracy, or improve the security of the OMS system.

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

VES is operating under the following examples of legal authority:

- Federal Information Security Management Act (FISMA)
- VA Directive 6500, VA Cybersecurity Program, and Handbook 6500, Risk Management Framework for VA Information Systems VA information Security Program
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Part 160

- 38 United States Code (U.S.C.) §§ 5721-5728, Veteran's Benefits, Information Security
- Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Systems
- 18 U.S.C. 641 Criminal Code: Public Money, Property or Records
- 18 U.S.C. 1905 Criminal Code: Disclosure of Confidential Information

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: Medium-An example being an insider threat to PII data.

Mitigation: Mitigation is complete and extensive through the following principles and solutions:

Principle of Purpose Specification: Under contractual and regulatory oversight the VA has provided the data necessary to perform the MDE process. The purpose of the data collection directly leads to billable MDEs and the completion of DBQs to establish veteran benefits. Internally the SSN is masked for employees so that this is not a risk.

Principle of Minimization: All case contact information and medical history are necessary for the case completion. Contact information is necessary to establish identity and complete exams. Medical history is necessary for the provider to establish any prior vs. service-created conditions. The minimum information needed is provided to employees per these examples above.

Principle of Individual Participation: Information from the veteran is provided to establish identity, establish symptoms and history for the DBQ exam process in a provider/patient relationship, and to personally correct any errors in the historic data.

Principle of Data Quality and Integrity: All policies and procedures, previously outlined, regarding data quality provide the most accurate and available data for the veteran. Data integrity is maintained through security procedures, policies, and systems including encryption at rest and in transit. Thumb drives are prohibited to protect PII data

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.

Contact information such as the Name, address, zip code, phone numbers, and Email address are used to establish the initial veteran contact and continued contact for scheduling. Information like the date of birth and/or SSN are used to validate the identity of the veteran and ensure data integrity. Medical records and current medication data is used to establish any conditions as part of the provider/patient exam. Metadata such as the IP address is used for security purposes.

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

The back-end database of Veterans Evaluation Services (VES) is a Microsoft SQL database, and many reports are used within VES for operational improvement only. Native SQL is used without a reporting server, data mart, or other data analysis services. No individual or aggregate information of individuals is performed for analysis for internal use or external consumption by a 3rd party.

On occasion VAROs have requested reports for their geographic area or case load for their area. In addition, reports for billing history and detail have been requested by the VA. VES has consistently provided data to these divisions of the VA as requested.

Internally data is collected regarding providers per area, provider specialties in a geographic area, case load by area, turn-around time for cases, wait time for providers, or other criteria to improve VES operations.

None of these reports utilize PHI or PII for individual veterans and are primarily tailored for improvement in operations. As a result, no reports would constitute any invasion into a veteran's privacy.

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?
FIPS140-2 encryption in transit and at rest. In transit using SSL and at rest using Self Encrypting Drives (SED)
2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
The VES user community uses Citrix servers in an isolated thin client environment. The Citrix isolated thin client environment prevents the VES user community from copying/stealing PHI/PII data while processing Exam Service Requests (ESR).
2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
VES has Data Lost Prevention (DLP) enabled on the VES email servers. DLP value is configured to prevent emailing of string values that resembles SSN and others flagged as PII.
All VES employees undergo mandatory annual corporate ethics and rules and behavior training to ensure they comply with protecting all VA data in accordance with VA Directive 6500. Data quality checks are completed through deployed on-premise automated tools that alerts the SOC of any changes or anomalies. The product features data profiling, data discovery and monitoring, as well as a 360-degree view that lets users uncover information about extended relationships within data. Workflow management functionality lets customers construct and modify workflows while hierarchy management enables a graphical display and navigational tools.

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.

Within the Veterans Evaluation Services system security controls exhibit the least-access rule of information in providing the minimum information necessary for VES employees to complete the requirements of their position. For the vast majority of our employees the majority of the PII is blocked from viewing. No SSNs are visible to the employee and more than 90% of the company does not have the permission to view full SSNs. In a tiny minority of cases VES has received incorrect SSNs and a minority of employees can override the SSN value within cases. Only employees previously approved by upper management within the call center have access to the full SSN. This is less than 10% of the company and approximately 10x individuals.

PHI data is relegated to each department as well on a least-access rule as well. Only the bookmarking, QA, and case builder teams can see PHI data while the Call center and many other departments cannot see any PHI data. This reduces the privacy risks to veterans as well.

A privacy statement is included in all documentation sent to veterans such as the paperwork behind a scheduled appointment whether Emailed or sent in printed form. This provides a clear statement to the veteran regarding the use of their PHI and PII data and the veteran's rights.

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 case information outlined in question 1.1 is retained within OMS for a 2 year plus case lifetime period. The case lifetime period is defined as the time it took to process a case. Medical records, or PHI, are also retained for the same time-period. The information is including:

- Name
- SSN
- DOB
- Mailing Address
- Zip Code
- Phone Number Version Date: November 2nd, 2018 Page 11 of 25
- Email Address
- Emergency Contact Info
- Internet Protocol (IP) Addresses
- Current Medications
- Prior Medical Records

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.

Per the contract, all case information and PHI are retained for a 3 year plus case lifetime period. The data lifetime is the case Over 95% of cases are processed in < 30 days with the remaining minority of cases typically processed in < 90 days. This makes the maximum time retention 3 years plus 90 days at most. The longest retention requirements are at most 4 years (1 year for the case + 3 years retention).

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.

VES uses the General Records Schedule 3.1 and 3.2 (GRS 20), approved by the National Archives and Records Administration (NARA) as our record retention and disposal schedule.

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

All SPI comprised of PHI and PII are automatically purged from the VES system via a record deletion on a 3 year plus 9- day cycle. PHI is archived after 1 year to tape and after 1 year the tape is purged or available to be overwritten. Both tapes and all storage is encrypted so data at rest is secure as well. Tapes are physically destroyed once this lifecycle is exceeded. In all cases automated SQL scripts or batch files delete the data in question.

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

Privacy Risk: The PII and PHI being separated by department, permissions structure, and physical placement already reduces the privacy risk to all retained cases and PHI. As a result, the

SPI risks are the same for a new case as well as a retained case which has been processed. Annual privacy and security training occurs for all employees working with cases.

Mitigation: Extensive encryption of production and archived/retained cases protects all data at rest including PII and PHI. Audit records within OMS outline any activity on any case so a full history of activity on an archived case can be built

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: Medium

Mitigation: The data purging processes are designed to be fully FIPPS compliant and to destroy all unnecessary data. Through keeping the minimum amount of data the minimum amount of time Veterans Evaluation Services works to fulfill the necessary data to complete a case and also protect the private information of our Veterans.

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***
Veterans Benefits Management System (VBMS) Exam Management System (EMS) via Data Access Service (DAS), Centralized Administrative Accounting Transactions System (CAATS)	Exam Requests are sent to the VES from VBMS via DAS. Results are sent back to VBMS via DAS. Decision Ready Claims (DRC) requests are sent via CAATS.	PII and PHI	Secure File Transfer Protocol (FTP) or XML packages

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: Medium-An example would be an employee attempting to abuse PHI/PII information through sharing with an unauthorized 3rd party (hackers, etc.).

Mitigation: The use of security groups, data protection from data leaks via Email, USB, etc., and encryption for all PHI/PII data are some of the basic measures. Internally, group-based controls allow PII/PHI scrubbing for the data views that the majority of the employees see, with a minority, where deemed appropriate, having access to PII/PHI data.

Secure test and development efforts use only scrubbed data for of all test/development data devoid of valid PHI/PII.

Finally, HR and IT driven policies and procedures outline the best practices for intra-company use of Veteran data. These cover the usage and training to prevent the leakage of any Veteran records.

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 information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	shared N/A	N/A	N/A	N/A

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: N/A-VES does not share data with external entities outside of the department.

Mitigation: N/A-VES does not share data with external entities outside of the department.

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.

As a contractor to the VA, all privacy acts are applicable to VES to implement in full. In addition, as a contractor to the VA all privacy notices are used within VES documents and grandfathered in use. VA privacy notices are posted within all physician forms for all Veterans utilizing VES services as a contractor for the VA.

Congress enacted Public Law 104-275, which authorized VA to contract for medical examinations from non-VA medical sources. The report stated a desire to see the contract medical examination authority expanded and made permanent. A subsequent contract was awarded under the same public law authority. The current contracts provided over 724,000 examination referrals during fiscal year 2017, and each referral, on average, results in 2-3 unique examination types, plus additional ancillary diagnostic services and Veteran travel benefits. This contract is anticipated to execute approximately of 7.7 million examination scheduling requests over the life of the 10-year contract.

Under VA awarded contract 36C10X19D0003 - project: Medical Disability Examinations (MDEs) under Section 504 of the Veterans' Benefits Improvements Act of 1996 (Public Law 104–275; 38 U.S.C. 5101) | Region 1 (Northeast) awarded to VES gives the authority to collect PII as documented in Title 38, United States Code, section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 34, 35, 36, 39, 51, 53, 55. The VA describes the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices. The SORN (58VA21/22/28) defines the information collected from Veterans and used in this system, and how the information is accessed and stored. The information collected is used to support the individual claim or claims the Veteran has been granted. VA SORN 58VA 21/22/28 is published at published at 84 FR 4138, November 8, 2021 and can be found at https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf and meets the federal requirements for notification. Further, VA public publishes a Privacy Act Statement and Notice of Privacy Practices on its public facing websites where individuals request services.

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

There is no penalty to decline information as all applicable information has been supplied by the VA as part of the case. PII is provided by the VA to VES with the initial case delivery. When verifying PII, all call center employees are instructed to correct or redact any PII that the Veteran electively chooses to. As long as VES can verify the identity of the Veteran, no other requirements exist to provide service to the Veteran and no penalties or denials of service will result.

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

The only use of PII information for VES is to perform a disability benefits questionnaire (DBQ) for the Veteran. With the initial contact from the call center the Veteran can choose to have his or her case returned to the VA. Yes, individuals can electively choose not to provide any PII to VES. If the case is returned then the data is deleted from VES systems.

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 only risks which exist are within a lack of clarity between the VA, the Veteran, and VES. The VA's privacy requirements are clearly outlined. The only risk is that the Veteran is unaware of the limits or extent of their privacy rights.

Mitigation: VES always works to communicate the rights and expectations to Veterans through forms. Additional training is planned for providers and additional information is planned to be released on the VES website

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.

Veterans may request access to Privacy Act records maintained by VA in writing. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VBA system of records, the Regional Office Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted. This process is outlined in the published SORN for the 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.

Veterans may request amendment to Privacy Act records maintained by VA in writing. All requests for amendment must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for amendment must be delivered to and reviewed by the Privacy Officer for the concerned VBA system of records This process for amendment of records outlined in the published SORN for the system.

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.

A request to amend any data contained in VA health records must be submitted in writing to the facility Privacy Officer, or designee, by the patient or Veteran stating explicitly what information is in contention and why, i.e., inaccurate or erroneous, irrelevant, untimely, or incomplete.").

This is guided by 38 CFR § 1.579 - Amendment of records.

(a) Any individual may request amendment of any Department of Veterans Affairs record pertaining to him or her. Not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date or receipt of such request, the Department of Veterans Affairs will

acknowledge in writing such receipt. The Department of Veterans Affairs will complete the review to amend or correct a record as soon as reasonably possible, normally within 30 days from the receipt of the request (excluding Saturdays, Sundays, and legal public holidays) unless unusual circumstances preclude completing action within that time. The Department of Veterans Affairs will promptly either:

(1) Correct any part thereof which the individual believes is not accurate, relevant, timely or complete; or

(2) Inform the individual of the Department of Veterans Affairs refusal to amend the record in accordance with his or her request, the reason for the refusal, the procedures by which the individual may request a review of that refusal by the Secretary or designee, and the name and address of such official.

(Authority: 5 U.S.C. 552a(d)(2))
(b) The administration or staff office having jurisdiction over the records involved will establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the Department of Veterans Affairs of an initial adverse Department of Veterans Affairs determination, and for whatever additional means may be necessary for each individual to be able to exercise fully, his or her right under 5 U.S.C. 552a.

(1) Headquarters officials designated as responsible for the amendment of records or information located in Central Office and under their jurisdiction include but are not limited to: Secretary; Deputy Secretary, as well as other appropriate individuals responsible for the conduct of business within the various Department of Veterans Affairs administrations and staff offices. These officials will determine and advise the requester of the identifying information required to relate the request to the appropriate record, evaluate and grant or deny requests to amend, review initial adverse determinations upon request, and assist requesters desiring to amend or appeal initial adverse determinations or learn further of the provisions for judicial review.

(2) The following field officials are designated as responsible for the amendment of records or information located in facilities under their jurisdiction, as appropriate: The Director of each Center, Domiciliary, Medical Center, Outpatient Clinic, Regional Office, Supply Depot, and Regional Counsels. These officials will function in the same manner at field facilities as that specified in the preceding subparagraph for headquarters officials in Central Office.

(Authority: 5 U.S.C. 552a(f)(4))
(c) Any individual who disagrees with the Department of Veterans Affairs refusal to amend his or her record may request a review of such refusal. The Department of Veterans Affairs will complete such review not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual request such review and make a final determination unless, for good cause shown, the Secretary extends such 30-day period. If, after review, the Secretary or designee also refuses to amend the record in accordance with the request the individual will be advised of the right to file with the Department of Veterans Affairs a concise statement setting forth the reasons for his or her disagreement with the Department of

Veterans Affairs refusal and also advise of the provisions for judicial review of the reviewing official's determination. (5 U.S.C. 552a(g)(1)(A))

(d) In any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (c) of this section, the Department of Veterans Affairs will clearly note any part of the record which is disputed and provide copies of the statement (and, if the Department of Veterans Affairs deems it appropriate, copies of a concise statement of the Department of Veterans Affairs reasons for not making the amendments requested) to persons or other agencies to whom the disputed record has been disclosed. (5 U.S.C. 552a(d)(4)) (38 U.S.C. 501)

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.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Any changes to the case are submitted back to the VA through the case completion via the VES clarifications department. If a Veteran requests changes to contact information, etc. this is handled by the VES call center Version Date: November 2nd, 2018 Page 19 of 25 after the Veteran's identity is established. If there are significant changes to the PII for the veteran this is sent by VES clarifications to the VA.

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: Most risks to PII and privacy are addressed under the framework of privacy protection and rights that the VA has created. Since VES does not originate the data, and since no information is shared with 3rd parties, VES does not have the risks associated with the creation or dissemination of PII or PHI data.

Mitigation: Existing steps outline the procedures to the call center employees of VES, which are the first line of Veteran communications. This and role-based security groups help secure the IT side of the PII management process. Per prior statements, the process and frameworks governing PII and PHI are defined under VA and NIST standards and followed by all VES employees. Furthermore, all employees must undergo annual PII training through the TMS process.

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.

All VES employees must undergo the hiring process and interview, a criminal background check, and successfully complete TMS training before their account is created. Accounts are created based upon defined templates so that permissions for an employee title flow through the system. Most employees see masked PII data with selected groups having access to the full PII data (also editing rights). These permissions are based upon the employee's business group and provide the least access necessary.

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.

VES is a contractor to the VA and no other contractors have access to any VA data under our control. The company does not hire contractors with access to production VA-supplied data and all employees fall under the previously outlined controls. TMS training for the employee and the prior ATO for the company are the clearances required.

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.

All users are required to annually complete VA Privacy and Information Security Awareness and Rules of Behavior training. This documentation and monitoring is performed using the Talent Management System (TMS).

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.***

VES operates under an ATO granted on 2/21/2020 and will expire 2/21/2023. All Continuous monitoring is met and compliant as of 11/16/2021.

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.

VES is an on-premise solution and is a private stand-alone cloud for the VA and operates under a full ATO granted 2/21/2021

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.

VA owns all rights to PII under contract order 36C10X19D0003. Executed on 03/19/2021

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.

None.

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.

Reference Section 15.2 - The Contractor's staff will have access to sensitive information contained in Veterans' records. The Contractor shall prevent the unauthorized release of information obtained by employees in the performance of work required by this contract. The Contractor shall ensure that employees are aware of and receive training, as necessary, on all regulations and laws such as the Privacy Act that restrict the release of information. Veterans' claims files, all examination reports, and all testing results are the property of VA, and the information contained therein is protected under the Privacy Act. All Veteran claims folders forwarded for copying/scanning must be maintained in locked files while under the care of the Contractor.

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).

None.

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
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**

ID	Privacy Controls
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.

Simon K. Caines 3430973

Digitally signed by Simon K. Caines 3430973
Date: 2022.02.03 12:33:29 -05'00'

Privacy Officer, Simon Caines

ANITA M. FEIERTAG 240557

Digitally signed by ANITA M. FEIERTAG 240557
Date: 2022.02.03 10:33:35 -05'00'

Information Systems Security Officer, Anita Feiertag

Jennifer L. Treger 105837

Digitally signed by Jennifer L. Treger 105837
Date: 2022.02.02 14:54:09 -05'00'

Information System Owner, Jennifer Treger

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).

- VA SORN 58VA 21/22/28 is published at published at 84 FR 4138, November 8, 2021 https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf
- https://www.va.gov/privacy-policy
- File for disability compensation with VA Form 21-526EZ | Veterans Affairs – Link to Privacy Act Statement on page