Privacy Impact Assessment for the VA IT System called:

Veterans Health Administration (VHA) Enrollment System (VES)

Enrollment Health Benefit Determination Program

Veterans Health Administration

eMASS ID 787

Date PIA submitted for review:

11 Dec 2023

System Contacts:

System Contacts

Role	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.katz-johnson@va.gov	203-535-7280
Information System Security Officer	Albert Estacio	Albert.estacio@va.gov	909-583-6309
Information System Owner	Athanasia Boskailo	athanasia.boskailo@va.gov	201-532-7923

Abstract

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

Veterans Health Administration (VHA) Enrollment System (VES) maintains and manages enrollment data so that Veterans can access healthcare benefits from the Veterans Health Administration.

The purpose of the VES database is to host demographic, and eligibility/enrollment information for all persons who interact with the VA's Enrollment and Identity Services applications. In addition to Veterans, healthcare providers – including direct care providers within and outside the VA, business office personnel, researchers, and management - require this administrative data to provide and improve healthcare delivery to Veterans. The VES database hosts the records of approximately 20 million individuals.

Overview

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

1 General Description

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

Veterans Health Administration (VHA) Enrollment System (VES). Owned by VHA

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

The VHA Enrollment System (VES) serves as the authoritative source on Veteran enrollment and eligibility. It encapsulates the functionality for enrollment and eligibility to allow Veterans to gain healthcare benefits from the Veterans Health Administration (VHA).

C. Who is the owner or control of the IT system or project?

VES is VA Owned and VA Operated. It is maintained as a VA Enterprise Cloud (VAEC) Amazon Web Service (AWS) system.

2. Information Collection and Sharing

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

The typical client is an individual that is eligible for and/or enrolled for healthcare benefits from the VHA. There are currently 21.7 million individuals stored within VES.

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

Information in the system corresponds to data needed to verify eligibility and enrollment status of an individual; such as name, contact information, gender, enrollment status, etc.

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

In the VA enterprise n-tier architecture, the VHA Enrollment System database serves as the data layer and its consuming/supporting applications make up the service layer. Data updates from the Health Eligibility Center (HEC) are synchronized with the VES database via messaging from the supported applications. VES enhances the operational efficiencies of HEC staff members and other staff at VA Medical Centers who coordinate changes to Veterans' eligibility.The system was previously known as Enrollment System Redesign (ESR) prior to moving to its current cloud environment and has retained the VA System Inventory (VASI) Identification (ID) number 1231.

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

VES is maintained as a VA Enterprise Cloud Amazon Web Service (VAEC AWS) system. All the security controls are implemented and adhere to Federal Risk and Authorization Management Program (FedRAMP) High compliance in all VAEC AWS Availability Zones. The live VES database is replicated constantly to a standby instance via Data Guard.

3. Legal Authority and SORN

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

The legal authority to operate this system comes from Veterans' Health Care Eligibility Reform Act of 1996, Public law 104-262

The SORN provides the following authority: Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

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

No modification of the System of Records Notice (SORN) is expected as a result of VES. The SORN was published, 17 Aug 2021. The SORN, "*Enrollment and Eligibility Records-VA*," (147VA10 / 86 FR 46090) can be accessed at https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

4. System Changes

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

No business processes will change as a result of this PIA. This PIA supports the data retention change approved in July 2022 – previous Veteran data was retained indefinitely. Data retention is being changed to seven (7) years following notification of the date of death of a Veteran; VES implementation is ongoing. This brings VES in alignment with the current SORN, "Enrollment and Eligibility Records-VA," (147VA10 / 86 FR 46090).

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

Technology changes are not expected outside of the above mentioned data retention.

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☒ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Gender
- ☒ Integrated Control Number (ICN)
- ☒ Military History/Service Connection
- ☒ Next of Kin
- ☒ Other Data Elements (list below)

Other PII/PHI data elements:

- Enrollment status
- Enrollment date

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

- Eligibility status
- Veteran associates [next of kin, family members, their contact information and dependent information (SSN, DOB, name, gender)]
- Marital Status
- Financial information [net income, net worth, gross income (for each year veteran enrolled)]
- Health Insurance [policy number, start date and card holder name]
- Medicaid Eligibility
- Veteran benefit information [VA Pension information and Service Connection Percentage (rated disabilities)]
- Veteran's preferred facility
- Veteran confirmation [whether individual exists]
- Nearest VA facility

PII Mapping of Components (Servers/Database)

VHA Enrollment System (VES) consists of eight key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VES and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A – no connections from VES components to other VA applications	N/A	N/A	N/A	N/A	N/A

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

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

Various VA internal services (see below).

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

Health Connect – Receives/Sends: Contains every data field in VES (see VES below).
Healthcare Application/VA.gov (HCA) – Receives: eligibility status, enrollment status, Veteran contact information, military service information, Veteran associates, financial

information, and health insurance. Sends: eligibility status, enrollment status, Veteran contact information, military service information, Veteran associates, and financial information.
SSN Verification- Sends a file via ConnectDirect containing: Name, SSN, DOB. Receives: Name, SSN, DOB, and verification status. Verification with Social Security Administration (SSA) on accuracy of SSN. Name, SSN, DOB. No direct connection maintained with SSA. Received information is sent to Enrollment Database Income Verification Matching Enrollment Database Income Verification Matching (EDB) which VES connects to (see section 4.1)
VA Profile- Sends*:* ICN, address, phone number, email. Receives: ICN, address, phone number, email. Maintain accurate veteran contact information from authoritative VA source. ICN, address, phone number, email.

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

The VHA Enrollment System – Does create information. It also receives/sends: Veteran Unique ID (ICN), enrollment status [success/rejection], enrollment date, eligibility status, Veteran contact information [address, phone number and e-mail addresses], military service information [branch of service, discharge type and discharge date], Veteran associates [next of kin, family members, their contact information and dependent information], financial information [net income, net worth, gross income for each year Veteran enrolled], health insurance [policy number, start date and card holder name], Veteran benefit information [VA pension information and service connection percentage (rated disabilities)], military history, Veteran's preferred facility, Veteran confirmation [whether individual exists] and nearest VA facility.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

All inputs to VES are from another system such as EDB, Hospital Inquiry (HNQ), and Healthcare Application (HCA). All information stored in the VHA Enrollment System database is sent to it electronically by the applications listed in Section 1.2.

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

VES is not submit to the Paperwork Reduction Act.

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

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

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that

receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

All inputs to VES are from another system such as Enrollment Database Income Verification Matching (EDB), Person Services Identity Management (PSIM), Healthcare Application/VA.gov (HCA) or HealthConnect. VES relies upon the initial system receiving the information to check the data for accuracy at the time of collection.

The VES database does not check the information provided to it for accuracy. It is the responsibility of the VA Enrollment and other applications which provide the information to the VES database to check the information for accuracy.

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

VES does not check for accuracy.

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

- Veterans' Health Care Eligibility Reform Act of 1996, Public law 104-262, Title I – Eligibility Reform, Sec 104 Management of Health Care
- Title 38, U.S. Code § 1705 Management of Health Care Patient Enrollment System: ''(a) In managing the provision of hospital care and medical services under section 1710(a) of this title, the Secretary, in accordance with regulations the Secretary shall prescribe, shall establish and operate a system of annual patient enrollment."
    - The VES database legal authority can be found also be found in Title 38, U.S. Code, Section 501 and Section 7304.
- The System of Records Notice (SORN), published 08/17/2021 is "Enrollment and Eligibility Records-VA" (147VA10), https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf and operate a system of annual patient enrollment." The SORN provides the following authority: Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Sensitive information including personal contact information, social security numbers or eligibility and enrollment information may be released to unauthorized individuals.

Mitigation: All employees with access to Veterans' information are required to complete the VA Privacy, Information Security Awareness training and Rules of Behavior annually.

Section 2. Uses of the Information

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

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

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.

- **Name:** Assists in uniquely identifying the person's information.
- **Mother's Maiden Name:** Assists in uniquely identifying the person's information.
- **Social Security Number (SSN):** Assists in uniquely identifying the person's information.
- **Date of birth:** Assists in uniquely identifying the person's information.
- **Address:** Assists in uniquely identifying the person's information.
- **Zip Code:** Assists in uniquely identifying the person's information.
- **Phone Number:** Assists in uniquely identifying the person's information.
- **Email Address:** Used to identify the person's patient records.
- **Race/Ethnicity:** Used to identify the person's patient records.
- **Integration Control Number (ICN**): Unique VA Identification (ID) number used across the enterprise.

- **Emergency Contact Information:** To share with clinical applications in case the veteran is hospitalized/dies inpatient.
- **Gender:** Assists in uniquely identifying the person's information.
- **Enrollment Status:** Determines if individual may receive health care benefits in VHA.
- **Enrollment Date:** Determines if individual may receive health care benefits in VHA.
- **Eligibility Status:** Determines if individual may receive health care benefits in VHA.
- **Branch of Service:** Used in determining eligibility status.
- **Discharge Type:** Used in determining eligibility status.
- **Discharge Date:** Used in determining eligibility status.
- **Next of Kin:** To share with clinical applications in case the veteran is hospitalized/dies inpatient.
- **Family Members:** For determining copay responsibilities; based on income thresholds and number of dependents.
- **Family Contact Information:** To share with clinical applications in case the veteran is hospitalized/dies inpatient.
- **Dependent Information:** Assists in identifying dependent(s)
- **Child's Date of Birth:** Assists in identifying dependent(s) or family member.
- **Child's SSN:** Assists in identifying dependent(s) or family member.
- **Child's Full Name and Gender:** Assists in identifying dependent(s) or family member.
- **Spouse Date of Birth:** Assists in identifying spouse.
- **Spouse SSN:** Assists in identifying spouse.
- **Spouse Full Name:** Assists in identifying spouse.
- **Marital Status:** Assists in identifying eligibility.
- **Medicaid Eligibility:** Assists in identifying eligibility.
- **Net Income:** Assists in identifying eligibility.
- **Net Worth:** Value is no longer collected though system retains historical data; it was previously used as a factor in determining copays.
- **Gross Income (for each year Veteran enrolled):** Assists in determining copay responsibilities.
- **Health Insurance Policy Number:** For potential third-party billing, VA may bill the private insurance instead of the veteran directly.
- **Health Insurance Start Date:** For potential third-party billing, VA may bill the private insurance instead of the veteran directly.
- **Health Insurance Card Holder Name:** For potential third-party billing, VA may bill the private insurance instead of the veteran directly.
- **Service Connection Percentage:** Disability rating for the person, used in determining eligibility status.
- **Military History:** Used in determining eligibility status.
- **Veteran's Preferred Facility:** Facility preferred by the veteran for receiving services.
- **Nearest VA Facility:** Nearest VA facility to send a Veteran to for treatment based on the provider's location.

2.2 What types of tools are used to analyze data and what type of data may be produced?

These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

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

For VES, the Member Services Informatics division performs data analytics and reporting to the VA in order to provide statistics on the Veteran enrollment population; statistics include growth rates, demographics, enrollment statuses and data anomalies. The Member Services Informatics division is external to the VES team and connects to the VES database for their analytic work.

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

Data stored in the VHA Enrollment System database is not analyzed and nothing is produced by the VHA Enrollment System database.

2.3 How is the information in the system secured?

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

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

The data is encrypted in transit and at rest in compliance with FIPS 199. SSN are encrypted.

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

SSN are encrypted.

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

The data is encrypted in transit and at rest in compliance with FIPS 199.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Users must be explicitly granted read permission through the LEAF process and approved by the supervisor and VES access group.

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

Documentation is maintained within the Access Control Standard Operating Procedures (SOP).

2.4c Does access require manager approval?

Users must be explicitly granted read permission through the LEAF process and approved by the supervisor and VES access group.

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

All records that users view or update are audited and logged by timestamp which record they have accessed. Every access is recorded in the database audit.

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

VES access group is responsible for creating, locking, and terminating application user accounts. VES DevSecOps team is responsible for safeguarding direct database access.

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

- Name
- Social Security Number (SSN)
- Date of birth
- Address
- Zip code

- Phone number
- E-mail address
- Integration Control Number (ICN)
- Emergency contact information
- Gender
- Enrollment status
- Enrollment date
- Eligibility status
- Branch of service
- Discharge type
- Discharge date
- Next of kin
- Family members
- Next of kin or family contact information
- Dependent information
- Net income
- Net worth
- Gross income (for each year Veteran enrolled)
- Health insurance policy number
- Health insurance start date
- Health insurance card holder name
- VA pension information
- Service connection percentage
- Military history
- Veteran's preferred facility
- Veteran confirmation
- Nearest VA facility
- HEC Collects: Name, Address, and Zip Codes on the letters that are mail

3.2 How long is information retained?

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

Records were maintained indefinitely. A change approved in July 2022 is being implemented that will result in Veteran records being destroyed 7 years after the income year for which the means test verification was conducted, when all phases of Veteran's appeal rights have ended. If an appeal is filed, the record is retained until all phases of the appeal have ended.

Generally, records will be maintained for 7 years after notification of the date of death of the Veteran.

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

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

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

Yes.

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

NARA approved GRS 3.2 Items 030, Ad-Hoc reports.

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

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

Records will be electronically deleted from all system databases at the end of the retention period. (This change has already been approved and is currently under technical review for date of implementation.) This is a scheduled change from the previous retention of records be retained indefinitely. Following deletion, any backups of the system with the data will be automatically overwritten within seven days.

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

For training and testing, only simulated data is used to ensure PII concerns are eliminated, and no unauthorized disclosure of information or misuse occurs. VES is not utilized for research purposes.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the information maintained by the VHA Enrollment System database could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk posed by information retention, the VES database adheres to the disposition authority approved by the Archivist of the United States. When the retention date is reached for a record, the individual's information is disposed of via approved electronic methods.

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***
HealthConnect	Proxy to all VA Medical Centers	Veterans' name, SSN, Date of birth, Address, Phone number, E-mail address, Emergency contact information, Health insurance information, Veteran unique ID, Gender, Enrollment status, Enrollment date, Eligibility status, Military service information, Veteran associates, Financial information, Health insurance, Veteran benefit information, Military history, Veteran's preferred facility, Veteran confirmation, Nearest VA facility, Mother's maiden name, Race/ethnicity, Spouse's full name, Child's full name and gender, Spouses date of birth, Child's date of birth, Spouse's SSN, Child's SSN, Current marital status, Medicaid eligibility, Annual income	Health Level 7 messages (HL7)

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*
Healthcare Application/VA.gov (HCA)	Public-facing interface for VES.	**Receives from HCA:** Eligibility status, Enrollment status, Veteran contact information, Military service information, Veteran associates, Financial information, Health Insurance **Sends to HCA:** Eligibility status, Enrollment status, Veteran contact information, Military service information, Veteran associates, Financial information	HCA Web Service and Enrollment and Eligibility (E&E) Web Service
Customer Relationship Management (CRM)	Relationship Management	Eligibility status, Enrollment status	E&E Web Service
Corporate Data Warehouse (CDW)	CDW retrieves records from the VHA Enrollment System database.	Veterans' name, SSN, Date of birth, Address, Phone number, E-mail address, Emergency contact information, Health insurance information, Veteran unique ID, Gender, Enrollment status, Enrollment date, Eligibility status, Military service information, Veteran associates, Financial information, Health insurance, Veteran benefit information, Military history, Veteran's preferred facility, Veteran confirmation, Nearest VA facility, Mother's maiden name, Race/ethnicity, Spouse's full name, Child's full name and gender, Spouses date of birth, Child's date of birth, Spouse's SSN, Child's SSN, Current marital	Direct Database Transfers

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*
		status, Medicaid eligibility, Annual income	
Person Services Identity Management (PSIM)	Causes VES to get an update on the ICN. Verify Veterans identity and retrieve the PII traits.	Veteran Unique ID (ICN), Veteran PII	Identity and Access Management (IAM)
Enrollment Database Income Verification Matching (EDB/IVM)	Veteran financial information exchange	Veteran PII, Eligibility status, Enrollment status, Veteran contact information, Military service information, Veteran associates, Financial information	E&E Web Service
Healthcare Claims Processing System (HCPS)	Veteran claims processing	Eligibility status, Enrollment status, Veteran contact information, Military service information, Veteran associates, Financial information	E&E Web Service
Nationwide Health Information Exchange (NwHIN)	Veteran's preferred facility	Veteran's preferred Facility	E&E Web Service
Veterans Identification Card (VIC)	Veteran Eligibility and enrollment information	Eligibility status, Enrollment status, Military service information	E&E Web Service
Veteran Information/ Eligibility Record Services (VRS or VIERS)	Veteran Eligibility and enrollment information	Enrollment status, Enrollment date	E&E Web Service
VA Profile	VA Profile retrieves records from the VHA Enrollment System database.	Veteran Identifier, address, phone, email	E&E Web Service

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Follow the format below:

Privacy Risk: The internal sharing of data is necessary, however, there is a risk that the data could be shared with an inappropriate VA organization or institution which could result in a breach of privacy and disclosure of PII/PHI to unintended parties or recipients.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized. Access to sensitive information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.

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***
Government Publishing Office; current vendor is News Printing Company (NPC)	Enrollment and Eligibility letter printing for Veterans	Veteran Unique ID (ICN), Veteran PII, Enrollment status, Veteran contact information, Military service information, Veteran associates, Financial information	Overseen by Government Print Office, ISA/MOU	Secure File Transport Protocol (SFTP)
Internal Revenue Service (IRS)	Transmit Veteran Health Coverage	Sent to IRS: First name, Last name, SSN, DOB, Address, Phone, Dates of coverage the individual was enrolled for VA health Received from IRS: Receipt identifier, Accept/Reject status, Error message (if applicable)	Transmission Control Code (IRS e-Services)	Simple Object Access Protocol (SOAP) Hypertext Transfer Protocol Secure (HTTPS)

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: VES sends a file to an external vendor for printing. Vendor selection is overseen by the Government Print Office (GPO). VES transmits data to the IRS.

Mitigation: The letters go to an external print vendor (determined by GPO) via SFTP but only contain name and address. Transmission is secured in transmission and then secured within the IRS systems handled under separate authorization boundaries.

Section 6. Notice

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

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

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

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

All of VES's data comes from other systems (HNQ, VIE, HCA, PSIM, and VDR) before reaching VES. The VHA Notice of Privacy Practice (NOPP) https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veteran. This Privacy Impact Assessment (PIA) also serves as notice As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means. "A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority and the conditions under which the information can be disclosed.

SOR Number: 147VA10 / 86 FR 46090

Title: Enrollment and Eligibility Records-VA
Publication Date: 17AUG21
Link: https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

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

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

The initial method of notification is in person during individual interviews or in writing via the Privacy Act statement on forms and applications completed by the individual. Additionally, the Department of Veterans Affairs also provides notice by publishing the following VA System of Record Notices (VA SORN) in the Federal Register and online.

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

The VHA Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter. This Privacy Impact Assessment (PIA) also serves as notice As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means. A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority and the conditions under which the information can be disclosed. Notice is provided in the SORN: If notice was provided in the Federal Register, provide the citation. SORN Full List of VA Privacy Act Systems of Records"

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.

Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them.

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.

Information is used, accessed, and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed, and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records. The NOPP is also available at all VHA medical centers from the facility Privacy Officer. The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

Section 7. Access, Redress, and Correction

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

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

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

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

All Veterans who are enrolled are mailed a Health Benefits handbook. The handbook includes such things as their benefits, factors that went into their enrollment decision, contact information for their medical facility and instructions for what to do if their information is incorrect.

Generally, individuals may update certain aspects of their information contained within VES via connected public facing websites which in turn, will update VES. An individual may also call the VA IAW the Health Benefits handbook and request a change be made where the VA staff would initiate the change directly on the individual's behalf.

In accordance with the System of records Notice for Enrollment and Eligibility Records-VA (147VA10), Individuals seeking information regarding access to and contesting of Enrollment and Eligibility Records may write to the Director, Health Eligibility Center, 2957 Clairmont Road, Atlanta, GA 30329.

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

VES is not exempt from the access provisions of the Privacy Act.

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

N/A, VES is a *Privacy Act* system.

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

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

Veterans receive a Health Benefit handbook when they are enrolled with the VA. The handbook provides instructions for the Veteran as to actions to take if information is incorrect. Generally, individuals may update certain aspects of their information contained within VES via connected public facing websites which in turn, will update VES. An individual may also call the VA IAW the Health Benefits handbook and request a change be made where the VA staff would initiate the change directly on the individual's behalf.

In accordance with the System of records Notice for Enrollment and Eligibility Records-VA (147VA10), Individuals seeking information regarding access to and contesting of Enrollment and Eligibility Records may write to the Director, Health Eligibility Center, 2957 Clairmont Road, Atlanta, GA 30329.

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.

Veterans receive a Health Benefit handbook when they are enrolled with the VA. The handbook provides instructions for the Veteran as to actions to take if information is incorrect.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Veterans are able to correct their information contained in VES. The VA Health Benefit Handbook provides instructions for the Veteran as to actions to take if information is incorrect.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that individuals will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: By publishing this PIA, the Notice of Privacy Practices and the applicable System of Records Notices, the VA makes the public aware of the information kept about Veterans. This document, the Notice of Privacy Practices and the System of Records Notices provide points of contact for members of the public who have questions or concerns about the applications and records.

Section 8. Technical Access and Security

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

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

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

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

Users request access to the application through the Health Eligibility Center (HEC) Access Request form and attest to being current on their annual VA Privacy, Information Security Awareness training and Rules of Behavior. The user's supervisor must sign their approval on the form and the user's Information Security Officer (ISO), after verifying the currency of the user training, signs their approval as well. The HEC ISO must also give approval for the user's access. Then the HEC ISO forwards the user's request to the VES application administrator for their account to be created.

Additional details on the procedures in place for users to access the VES are contained within the VES Access Controls Standard Operating Procedures document.

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

Non-VA users will not have access

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

The VES Access Controls Standard Operating Procedures document describes the different accesses that may be granted to a user in depth. Generally, there are Read-Only and Elevated Privilege accounts. All accounts are created in accordance with the approved LEAF request.

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Per specific contract guidelines, contractors can have access to the system only after completing mandatory information security and privacy training, VA Health Insurance Portability and Accountability Act (HIPAA) training as well as the appropriate background investigation to include fingerprinting. Certification that this training has been completed by all contractors must be provided to the Information Security Officer (ISO). VA contractors access VES and HEC; the majority of the development team is comprised of contractors. The System Administrator team is also comprised of contractors. Access to the system for both teams is required for ongoing software development work to continue as well as for day-to-day maintenance of the system and its network.

Review of access to VES systems is done on a periodic basis determined by access type or role. Clearance is required for each person accessing the system. Each contract is reviewed prior to approval based on the contract guidelines by the appropriate contract authority (i.e., COR, Contracting Officer, Contract Review Committee, Technical Representative). Contracts are reviewed annually by the contracting authority.

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 VA users receive annual Privacy and Security Awareness training detailing appropriate and inappropriate use of Personally Identifiable Information (PII) and Protected Health Information (PHI). VES and HEC users receive virtual training that is offered monthly and tracked through the VA Talent Management System (TMS). The training consists of a three-hour online meeting facilitated by an instructor.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 14 Nov 2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 30 Mar 2023
5. *The Authorization Termination Date:* 29 Mar 2024
6. *The Risk Review Completion Date:* 21 Mar 2023
7. *The FIPS 199 classification of the system:* High

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

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

N/A.

Section 9 – Technology Usage

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

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

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

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

The system uses cloud technology, VAEC AWS.

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

VAEC – N/A.

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.

VAEC – N/A.

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.

VAEC – N/A.

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).

N/A.

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

ID	Privacy Controls
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**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2024.01.16 14:57:36 -05'00'

Privacy Officer, Nancy Katz-Johnson

ALBERTINO ESTACIO

Digitally signed by ALBERTINO ESTACIO
Date: 2024.01.12 14:17:13 -08'00'

Information System Security Officer, Albert Estacio

ATHANASIA BOSKAILO

Digitally signed by ATHANASIA BOSKAILO
Date: 2024.01.10 12:58:51 -05'00'

Information System Owner, Athanasia Boskailo

APPENDIX A-6.1

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

VHA Notice of Privacy Practice:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3147

SOR Number: 147VA10 / 86 FR 46090

Title: Enrollment and Eligibility Records-VA

Publication Date: 17AUG21

Link: https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

HELPFUL LINKS:

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

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

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

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

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