Privacy Impact Assessment for the VA IT System called:

Occupational Health Record-Keeping System (OHRS) 2.0

Veterans Health Administration (VHA)

Office of Information and Technology (OIT), Health Services Portfolio, Healthcare Environment and Logistics Management (HELM) Product Line

eMASS ID #1934

Date PIA submitted for review:

05/22/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.Katz-Johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842-2000X4613
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-595-7291

Abstract

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

The Occupational Health Record-Keeping System (OHRS 2.0) provides Employee Occupational Health (EOH) staff the ability to create, maintain, and monitor medical records for VA employees including the ability to generate site-specific reports at the National, Veterans Integrated Service Network (VISN), and facility levels. OHRS 2.0 include features that address EOH needs such as: COVID-19 Crisis Tracking Module, Integrations with HR smart (employee demographics), Role-based access control, Migration of Data from Legacy Product, Adherence with VA Security and Privacy Requirements, and Reporting Vaccinations/Immunizations/Immunity.

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?
Occupational Health Record-Keeping System (OHRS 2.0), Office of Information and Technology (OIT). Health Services Portfolio, Healthcare Environment and Logistics Management (HELM) Product Line

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 Occupational Health Record-Keeping System (OHRS) 2.0, Veterans Health Administration is the selected solution to provide all EOH staff with features such as documentation, forms, and tracking. This solution automates EOH process and data elements that are currently being manually tracked in a spreadsheet. OHRS 2.0 is used to provide care to 600,000 VHA Occupational Health employees who are responsible for providing care to Veterans and other VA employees.

C. Who is the owner or control of the IT system or project?
Healthcare Environment and Logistics Management (HELM) Product Line

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?
OHRS 2.0 stores information for over 450,000 VA Employee Occupational Health (EOH) employees and includes employee demographics, vaccination tracking, employee health documentation, forms, and mandatory health reports.

E. What is a general description of the information in the IT system and the purpose for collecting this information?
Occupational Health Record-Keeping System 2.0 (OHRS 2.0) ensures Occupational Health Staff have a fully operational system in which employee occupational health regulations and standards are tracked through the ability to create, maintain, and monitor medical records for VA medical employees and generate site-specific reports. The automated, secure solution improves data

accuracy through the use of automated error checking in data entry and reduces the time to enter the medical information.

e

F. What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.
Human Resource – Payroll Application Services (HR-PAS) transmits one way employee demographics data via Digital Transformation Center (DTC) Integration Platform (DIP) interface with OHRS 2.0.

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?*
OHRS 2.0 will be managed and maintained from the Salesforce Government Cloud Plus-Enterprise (SFGCP-E) sites located with the Amazon Web Services (AWS) GovCloud (West) region as specified in the SFGCP Salesforce PIA. The specific security controls leveraged by VA Salesforce, in addition to a detailed description of the SFGCP /Salesforce security boundaries, are documented in the VA SFGCP System Security Plan (SSP). OHRS 2.0 is one of several modules hosted on the Salesforce Government Cloud Plus (SFGCP) platform.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?
• VA SORN#08VA05 Employee Medical File Systems of Records (Title 38)-VA
• Employee Medical File Systems of Records (OPM/GOVT-10) for Title 5 employees
• Executive Orders 12107, 12196 and 12564; Urgent Relief for the Homeless Supplemental Appropriations Act of 1987, Public Law 100–71, Section 503, 101 Stat. 468 (1987); 38 U.S.C, Chapter 3, §§501(a)–(b); Chapter 73 and Chapter 75, §7802; 5 U.S.C Chapters 11. 33, and 63.

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?
SORN for this system is #08VA05 and OPM/GOVT-10
https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf 2023-01438.pdf (govinfo.gov) - 08VA05 OPM_GOVT.pdf (sharepoint.com)
The SORN does not need to be updated.

4. System Changes

J. Will the completion of this PIA will result in circumstances that require changes to business processes?
No

K. Will the completion of this PIA could potentially result in technology changes?
No

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: Additional SPI received from the HRIS system: Gender, job position, employee ID and occupational health information for Occupational Safety and Health Administration (OSHA) compliance.

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

PII Mapping of Components (Servers/Database)

OHRS 2.0 consists of 1 key component. The component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by OHRS 2.0 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
HR-PAS	Yes	Yes	Social Security Number, name, e-mail, address, gender, DOB, job position, employee ID	Information is used to track individuals (employees) who are receiving vaccinations for diseases such as the COVID-19 virus or influenza.	Data will not be transmitted to non-VA storage.
BISL_OHRS	No	Yes	Social Security Number, name, e-mail, address, gender, DOB, job position, employee ID	The BISL_OHRS database, in the CDW Occupational Health workspace, was set up to pull COVID vaccine data from OHRS 2.0.	Data will not be transmitted to non-VA storage.

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?
Human Resource Information System Shared Service Center (HRIS SSC) HR-PAS Database: Integration with HR-PAS database will provides employee Social Security Number, name, e-mail, address, gender, DOB, job position, employee ID.

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.
The other sources are required because OHRS 2.0 requires the information that HRIS and HR-PAS stores to use for identifying employees.

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

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?

An MOU has been established between HRIS SSC and VA OI&T EPMD Health regarding the development, management, operation, and security of a connection between HR·SMART (HR-PAS database), owned by HRIS SSC, and OHRS 2.0. The information from the HR-PAS is transmitted one way to OHRS 2.0 via flat file and web service API. All data is encrypted during this collection process.
Initial employee data is "pre-loaded" into OHRS 2.0. Once data is pre-loaded, data is sent via a flat file and web service API on a daily interval.
For user-provided data: via data typed into on-screen forms
Reference: SFGCP-E control implementation statement CA-09 Internal System Connections for details.
Information is also collected directly from individuals.

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?
Information is not collected on a form and subject 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.
The employee demographic information retained in the system is received directly from the authoritative source which is HRIS SSC via a flat file and/or API. Information accuracy is conducted at the point of service with the patient by Occupational Health Staff as part of the business workflow and information management. The procedure to update inaccurate or erroneous employee information, i.e spelling of names, date of birth, social security number, in OHRS 2.0 requires requests go through Human Resources.

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?
No

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

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under 45 CFR § 164.502 (3) and 45 CFR § 164.510.
•VA SORN#08VA05 Employee Medical File Systems of Records for Title 38 Employees Federal Information Security Management Act of 2002, 44 U.S.C. 3541 et seq
(FISMA, Title III of the E-Government Act of 2002, 44 U.S.C. 101)
•Employee Medical File Systems of Records (OPM/GOVT-10) for Title 5 employees
•Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Part160

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information
Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*
Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.
Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?
Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?
Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.
Follow the format below when entering your risk assessment:
Privacy Risk: If appropriate safeguards are not in place, the Sensitive Personal Information (SPI) including personal contact information, SSN and medical information may be compromised and release to unauthorized individuals.
Mitigation: The OHRS 2.0 application adheres to information security requirements instituted by the VA Office of Information Technology (OIT). OHRS 2.0 receives the data from VA Authoritative Data Sources authorized to collect and transmit the data. OHRS 2.0 will be hosted in the SFGCP which is rated at System Categorization Level HIGH and the data is stored in a FedRAMP certified HIGH environment protected by HIGH level security controls. SFGCP implements cryptography that is compliant with federal laws and regulations i.e., FIPS 140-2. All PII data is encrypted during transport and encrypted at rest. Profile based permissions will govern what access users have access to.

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.

PII/PHI Data Element	Internal Use	External Use
Social Security Number	Used as a unique identifier (for employees, volunteers & clinical trainees)	Not used
Name	Used as an identifier (for employees, volunteers & clinical trainees)	Not used
Date of Birth	Used as an identifier (for employees, volunteers & clinical trainees)	Not used
Mailing Address	State and Zip Code are used as an identifier	Not used
Medical Records	Application is used to record and store immunization and medical clearance records	Not used
Race/Ethnicity	Informational	Not used
Gender	Informational	Not used
Job Position	Informational	Not used
Employee ID	used as a unique identifier by the HR-PAS integration to match data with importing updated employee data.	Not used
Health Information	Application is used to record and store immunization and medical clearance records	Not used

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?

Information collected is utilized by Authentication and Authorization (A&A) services of Active Directory (AD) and "Modules" applications in both the pre-production/production environments. OHRS 2.0 does not perform data analysis or create data from data analysis. Derived data is displayed to users in actionable reporting formats. It is not stored and not attached to an individual's record.

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.

Information collected is utilized by Authentication and Authorization (A&A) services of Active Directory (AD) and "Modules" applications in both the pre-production/production environments. OHRS 2.0 does not perform data analysis or create data from data analysis. Derived data is displayed to users in actionable reporting formats. It is not stored and not attached to an individual's record.

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?

Data in transit is protected using Transport Layer Security (TLS) 1.2/1.3. Data is encrypted at rest using Salesforce Shield encryption and only able to be accessed by users with explicit need to view it.

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

The SSNs are encrypted at rest using Salesforce Shield encryption and only able to be accessed by users with explicit need to view them.

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

In addition to technical safeguards, there are administrative safeguards to include policies in place to prevent the circumvention of least privilege, role-based access controls, and need to know principles. All personnel are required to complete VA Privacy and Information Security Awareness and Rules of Behavior web-based training and Privacy and HIPAA training. Privileged users are required to complete Information Security and Privacy Role-Based Training for System Administrators web-based training. All users must sign the Rules of Behavior (ROB) agreeing to responsibilities and expected behavior for use of VA information and information systems.

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?

OHRS 2.0 follows the need-to-know principle of only granting access to the data users need to perform the functions of their official duties. OHRS 2.0 users are put into security roles based on job position that determines level of access to PII. All personnel with access to VA IT systems are appropriately cleared and qualified under the provisions of VA policy.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?
OHRS 2.0 access is limited to VA personnel who have been trained, vetted, and cleared via the personnel security process. VA employees with access to information on OHRS 2.0 are required to complete VA, 10176, VA Privacy and Information Security Awareness and Rules of Behavior (WBT), VA, 10203, Privacy and Health Information Portability and Accountability Act (HIPAA) Training annually, and appropriate OHRS 2.0 training if assigned a role other than Employee. Personnel must successfully obtain a Public Trust clearance.

2.4c Does access require manager approval?
Default access is established when HR-Feed synchronizes with OHRS 2.0 which automatically creates a user account(s). OHRS 2.0 users must have a VA network account for user(s) to login with single sign-on. VA users accessing OHRS 2.0 will go through the formal VA access request process, which requires supervisor/manager approval before access is granted to network applications.

2.4d Is access to the PII being monitored, tracked, or recorded?
Activity logs are available containing the required metadata to identify who, what, when, where, and how PII data was accessed.

2.4e Who is responsible for assuring safeguards for the PII?
All users of the system are responsible for safeguarding PII. The system administrators are responsible for assigning users to the appropriate user roles to limit access and assure PII safeguards as documented in the technical documentation and system design documentation.

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, e-mail, address, gender, DOB, job position, employee ID

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.*

VA will retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule. OIT retains audit records for a defined time-period to provide support for after-the-fact investigations of security incidents and to meet regulatory and VA information retention requirements. A minimum of 1 year or as documented in the NARA retention periods, HIPAA legislation (for VHA), or whichever is greater. Audit logs which describe a security breach must be maintained for 6 years (HIPAA requirement).

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?

The records are maintained in Employee Medical File Systems of Records (OPM/GOVT-10) for Title 5 employees and VA 08VA05 for Title 38 employees which authorize various routine use disclosures without the employee's written release of information or authorization. All records created in OHRS shall be managed according to the National Archives and Records Administration (NARA), General Records Schedule (GRS) 1, Civilian Personnel Records, Items 21 &34, and VHA Records Control Schedule (RCS) 10-1SFGCP records are retained according to NARA Record Control Schedule 10-1 (reference: https://www.archives.gov/).

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

This system complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records contained in the Salesforce FedRAMP cloud will be retained in accordance with a NARA-approved retention period.

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.

Salesforce Government Cloud Plus-Enterprise (SFGCP-E) follows VA Handbook 6300.1, "Records Management Procedures. Electronic data and files of any type, including PII, PHI, SPI and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Media Sanitization (January 23, 2019). When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. In the event data extension is unused for six (6) months, then the cloud-hosted regulations, Salesforce Data Retention Policy will be implemented as needed. Salesforce Government Cloud commits to removing data entirely from their systems within six (6) months after archiving/end of contract.

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.

No PII/live data is used for training, testing, or research. All internal employees with access to employee's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

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: If information is retained longer than specified, privacy information may be released to unauthorized individuals.

Mitigation: The risk associated with the length of time the data is retained is considered minimal. All data at rest within the SFGCP security boundary is encrypted in accordance with FIPS 140-2, as well as protected by FedRAMP certified "HIGH" security controls. Use of FedRAMP HIGH controls implemented under the FedRAMP ATO. Collectively, these controls within the SFGCP security boundary provide maximum protection to all VA Salesforce data. SFGCP only retains the required relevant information relevant as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedul

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***
Human Resource Information System Shared Service Center (HRIS SSC)	The purpose of the information being shared/received is VA employee occupational health tracking, compliance and improvement. This information will be used to ensure that VA employees have all of the occupational health safety measures they need to serve veterans safely and securely.	Social Security Number, Name, Email Address, Physical Address, Gender, Date of Birth, Job Position, Employee ID	Flat file, web service API
Digital Veterans Platform (DVP)	The purpose of the information being shared/received is VA employee occupational health tracking, compliance and improvement. This information will be used to ensure that VA employees have all of the occupational health safety measures they need to serve veterans safely and securely.	Social Security Number, Name, Email Address, Physical Address, Gender, Date of Birth, Job Position, Employee ID	Flat file, web service, API
Corporate Data Warehouse (CDW)	The purpose of the information being shared/received is VA employee occupational health tracking, compliance and improvement. This information will be used to ensure that VA employees have all of the occupational health safety measures they need to serve veterans safely and securely.	Social Security Number, Name, Email Address, Physical Address, Gender, Date of Birth, Job Position, Employee ID, Vaccination Status	Flat file, web service, API

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 for individuals to receive VHA benefits, 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 within the facilities. 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***
N/A	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.

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: Not applicable, as there is no sharing of information outside of Salesforce or VA with external partners.

Mitigation: Not applicable, as there is no sharing of information outside of Salesforce or VA with external partners.

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.
The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
explains the collection and use of protected health information to individuals receiving health care from VA
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."
Notice is also provided in the Federal Register with the publication of the SORN.

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.
Notice is given, see above. The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
explains the collection and use of protected health information to individuals receiving health care from VA

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 SORN, PIA, and Privacy Act Statement describes how patient health information may be used and shared. It also outlines privacy rights, including the right to complain if they believe their privacy rights have been violated.

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.
Individuals/Veterans have the right to decline to provide their information; however, without providing the information cannot originate a specific Module case record under the OHRS 2.0 application.

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.
Individuals do not have the option to decline to provide information for specific uses to the source VA 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. (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 EOH staff and employees may not be familiar with OHRS 2.0 and it uses within the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk by providing an Employee Occupational Health (EOH) Training SharePoint site that contains Talent Management System (TMS) links (TMS training course #43340) and quick reference guides that provides training and guidance to all staff and users across the VA. Users are required to take the final assessment and earn at a 70% before they are given access to the system.

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.***
Title 38 employees are under SORN 08VA05 – record access procedures: Individuals requesting access to and contesting the contents of records must submit to the Human Resources Management Office at the facility where last employed the following information for their records to be located and identified: (1) Full name, (2) date of birth, (3) last four of social security number, (4) name and location of VA facility where last employed and dates of employment, and (5) signature.
Title 5 employees are under SORN OPM/GOVT–1: RECORD ACCESS PROCEDURE: Individuals wishing to request access to their records should contact the appropriate OPM or agency office, as specified in the Notification Procedure section. Individuals must furnish the following information for their records to be located and identified: a. Full name(s). b. Date of birth. c. Social security number. d. Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees). e. Signature. Individuals requesting access must also comply with the Office's Privacy Act regulations on verification of identity and access to records (5 CFR part 297).

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)?
OHRS 2.0 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?
OHRS 2.0 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.
The procedure to update inaccurate or erroneous employee information, i.e spelling of names, date of birth, social security number, in OHRS 2.0 requests should go through Human Resources. To update inaccurate vaccination records, The OHRS 2.0 Administrator, assigned to each facility, should be engaged to update. An approval process within the module is completed. When a record is approved for correction, the data is serialized and moved into the archive object, and the record, immunization or immunization dose, is hidden in the system. If any-one needs the data from the original record, the data can be retrieved and re-instated in a new record.

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.
The OHRS 2.0 Administrator, identified for each facility, can guide users to seek corrections via Human Resources. This is also identified in this PIA and the SORN

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.
OHRS 2.0 allows users to directly view their records and for updates to their personal information, seek guidance from Human Resources. All HR data is to come from the integration to HR-PAS.

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: If individuals are not provided sufficient guidance regarding the access, redress, and correction of their data, then individuals could initiate adverse personnel actions against the Government.
Mitigation: By publishing this PIA, VA makes the public aware of methods for correcting their records. Because this system does not hold authoritative records long-term, it is unlikely individuals will feel the need to correct their information in this system Section 8. Technical Access and Security.

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?
The OHRS 2.0 application is accessible to internal users who require logical access to VA information services/applications. Account creation is managed and offered through VA via Single Sign On internal (SSOi) and two factor authentication (2FA) Personal Identity Verification (PIV) card.

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?
OHRS 2.0 does not have users from other agencies with access to the application.

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.

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.
The Salesforce Digital Transformation Center (DTC) contractor team supports the VA Salesforce production environment and as such has access to the OHRS 2.0 system and data contained therein. The Contractor and its employees, as appropriate, shall be required to sign Non-Disclosure Agreements (NDA). This includes PII and VA Sensitive Information. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior training via the VA's Talent Management System (TMS). Crystal Moultrie serves as the VA Contract Officer's Representative (COR) for the Salesforce DTC contract and Michael Domanski is the VA Salesforce System Owner. Mr. Domanski maintains governing authority over all VA Salesforce environments. The Salesforce DTC team will maintain users, update applications and components, introduce new functionality, govern deployment activities and ensure user operability. The Salesforce DTC members are not primary users VA Salesforce. Mr. Domanski will monitor and review VA Salesforce related support contracts on a regular basis to ensure no gaps in support for the platform and community users. Developers do not have access to production PII.

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.
As an action under the Continuous Readiness in Information Security Program (CRISP), VA's Assistant Secretary for Information and Technology issued a memorandum requiring all VA government and contract staff to complete information security awareness and applicable role-based training. All VA government and contract staff are required to complete information security awareness and applicable role-based training and maintain Talent Management System (TMS) Training Certificates of completion for VA Privacy and Information Security Awareness (PISA), Rules of Behavior (ROB), Health Insurance Portability and Accountability Act (HIPAA). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS 2.0 system.

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

8.4a If Yes, provide:

1. *The Security Plan Status: Approved*
2. *The System Security Plan Status Date: 25-May-2023*
3. *The Authorization Status: ATO*
4. *The Authorization Date: 25-Jul-2023*
5. *The Authorization Termination Date: 24-Jul-2025*
6. *The Risk Review Completion Date: 17-Jul-2023*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH): High*

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

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

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)*

Government Cloud - Salesforce Government Cloud Plus (SFGCP), Org-VHA-GOV

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.*

Service Provider: Contract entitled: "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B, Order Number: 36C10B9F0460.

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

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

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

The CPS will not collect any ancillary data.

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.

There are no contracts with customers for this application.

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

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

The system does not utilize Robotics Process Automation.

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**
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: 2024.09.03 13:48:32 -04'00'

Privacy Officer, Nancy Katz-Johnson

JAMES BORING

Digitally signed by JAMES BORING
Date: 2024.08.26 08:29:14 -04'00'

Information System Security Officer, James Boring

MICHAEL DOMANSKI

Digitally signed by MICHAEL DOMANSKI
Date: 2024.08.23 11:23:30 -04'00'

Information System Owner, Michael Domanski

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).

Link to the Privacy Policy found https://www.va.gov/privacy-policy

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

1605.04 Notice of Privacy Practices