Privacy Impact Assessment for the VA IT System called:

eSolution for Health care and Occupational Recordkeeping of Employees (eSHORE)

Veterans' Health Administration (VHA)

Healthcare Environment and Logistics Management

eMASS ID # 2425

Date PIA submitted for review:

08/08/2024

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)	Robert Gaylor	Robert.gaylor@va.gov	303-478-6558
Information System Owner (ISO)	Dr. Aaron Drew	Aaron.drew@va.gov	202-461-4363

Abstract

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

eSHORE provides all VHA Employee Occupational Health (EOH) staff with a standardized, comprehensive electronic health record (EHR) solution, allowing EOH staff to document, monitor, track, and maintain all employee occupational health services for VA personnel and generate site-specific reports at the national, Veterans Integrated Service Network (VISN), and facility level.

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?

The Information Technology (IT) system is eSolution for Health Care and Occupational Recordkeeping of Employees (eSHORE). The program office that owns the IT System is Healthcare Environment and Logistics Management.

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

VHA EOH staff utilize eSHORE to document all occupational health services including, but not limited to, administrative examinations, medical surveillance, work-related injury and illnesses, safety interventions, vaccinations, prevention and management of infectious diseases, and health promotion activities. The eSHORE application supports the employee occupational health program office and VA mission by providing modules such as patient encounters and history, medical surveillance, respirator medical clearance, mass immunization program management, scheduling, analytics, electronic signatures, and more to the enterprise.

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

VA Owned and VA Operated.

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?

eSHORE will be used to provide occupational health services to 400,000 VA employees who are responsible for providing care and support to Veterans and other VA employees.

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

Information in eSHORE consist of administrative examinations, medical surveillance, work-related injury and illnesses, safety interventions, prevention and management of infectious diseases, and health promotion activities. EOH information is collected to document, monitor, track, and maintain all employee occupational health services for VA personnel and generate site-specific reports at the national, Veterans Integrated Service Network (VISN), and facility level.

F. What information sharing is 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 eSHORE. VA Microsoft Active Directory Azure Assessing (Entra ID) and eSHORE bidirectionally transmits authentication, and authorization information with each other.

G. Is the system 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?

eSHORE is only operated in Veterans Affairs Enterprise Cloud (VAEC) which is in Amazon Web Services (AWS) GovCloud High.

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 Order 12107, Federal Civil Service Reorganization
• Executive Order 12196, Occupational Safety and Health Programs for Federal Employees
• 5 U.S.C, Government Organization and Employees, Chapter 11, Office of Personnel Management
• 5 U.S.C, Government Organization and Employees, Chapter 33 Examination, selection, and placement
• 5 U.S.C, Government Organization and Employees, Chapter 63, Leave

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?

An update to SORN is not necessary.

4. System Changes

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

No, this PIA will not require changes to business processes.

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

No, this PIA will not result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Other PII/PHI data elements:

Work Email Address, Employee ID, Job Position

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

PII Mapping of Components

eSHORE consists of **3** key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **eSHORE** 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, Application, 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
AmazonRDS (Relational Database Service)	Yes	Yes	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact Information • Medications • Medical Records • Race/Ethnicity • Medical Record Number • Gender	Information is collected for the provision of medical care and follow-up. Provide data necessary for proper medical evaluations and diagnoses, to ensure that proper treatment is administered, and to maintain continuity of medical care.	Network isolation with system located in virtual private cloud. Data at rest protection using Advanced Encryption Standard (AES) 256. Database encryption uses Amazon Web Services Key Management Services (AWS KMS). Only accessible to individuals with a need to know.

			• Work Email Address • Employee ID • Job Position		
eSHORE (Web Application)	Yes	No	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact Information • Medications • Medical Records • Race/Ethnicity • Medical Record Number • Gender • Work Email Address • Employee ID • Job Position	Information is collected for the provision of medical care and follow-up. Provide data necessary for proper medical evaluations and diagnoses, to ensure that proper treatment is administered, and to maintain continuity of medical care.	Network isolation with system located in virtual private cloud. Data at rest protection using Advanced Encryption Standard (AES) 256 and data in transit using Hypertext Transfer Protocol Secure (HTTPS) encryption. Only accessible to individuals with a need to know.
File System (Amazon S3 Bucket)	Yes	Yes	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address	Information is collected for the provision of medical care and follow-up. Provide data necessary for proper medical evaluations and diagnoses, to ensure that	Data at rest protection using Advanced Encryption Standard (AES) 256. Only accessible to individuals with a need to know.

			• Emergency Contact Information • Medications • Medical Records • Race/Ethnicity • Medical Record Number • Gender • Work Email Address • Employee ID • Job Position	proper treatment is administered, and to maintain continuity of medical care.	

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?

Records in eSHORE are obtained from the individual to whom the records pertain, VHA employee occupational health staff, and HR-PAS.

HR-PAS will provide employee Social Security Number, name, work e-mail address, personal mailing address, gender, DOB, job position, employee ID, and Ethnicity/Race. Integration with VA Microsoft Active Directory Azure Assessing (Entra ID) will reference employee names and work email addresses for authentication. VHA occupational health employees' update and maintain employee health information in their employee medical record.

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 VA Microsoft Active Directory Azure Assessing (Entra ID) integration is required for identification and authentication. The Entra ID Security Assertion Markup Language (SAML) attribute passes the authentication username and email address to the Service Provider (SP) to make authorization decisions about the user's access to eSHORE. Information from HR-PAS is required to retrieve VA personnel demographic data to create and update employee health records in eSHORE. Demographic data from HR-PAS is the source for employee's demographic data in eSHORE.

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

Yes, eSHORE can create custom reports for users.

1.3 How is the information collected?

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

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

Information is collected directly from employees.

EOH Staff perform examinations, vaccinations, and other occupation health services on employees and enter data into eSHORE via appropriate module forms.

Information is transmitted from HR-PAS to eSHORE via HTTPS.

Entra ID authentication information, attributes, and authorization decision statements are transmitted via Lightweight Directory Access Protocol over Secure Socket Layer (SSL)(LDAPS), Security Assertion Markup Language (SAML), HTTPS to eSHORE.

Specific eSHORE users have the capability to run pre-configured or custom generated reports from the data stored in the system.

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 Human Resources (HR)-feed via HR-PAS will insert new records and update existing records with PII data on scheduled intervals of daily for changes (deltas), and bi-weekly for the full load. The procedure to update inaccurate or erroneous employee information, i.e., spelling of names, date of

birth, social security number, in eSHORE requires requests to go through Human Resources. Health 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.

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

• 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 Order 12107, Federal Civil Service Reorganization
• Executive Order 12196, Occupational Safety and Health Programs for Federal Employees
• 5 U.S.C, Government Organization and Employees, Chapter 11, Office of Personnel Management
• 5 U.S.C, Government Organization and Employees, Chapter 33 Examination, selection, and placement
• 5 U.S.C, Government Organization and Employees, Chapter 63, Leave

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, last four of SSN and medical information may be compromised and released to unauthorized individuals.

Mitigation: Data received is from VA authoritative data sources authorized to collect and transmit the data. eSHORE is hosted in VAEC AWS, which is an AWS GovCloud environment that is rated System Categorization Level HIGH and the data stored in the environment is protected by HIGH level security controls. All PII/PHI data is encrypted during transmission and at rest. Access to the application is restricted to VA employees with Personal Identification Verification (PIV) card for multifactor authentication. Role-based access control is utilized to provide users with access to only the information needed to perform the duties of their role.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Social Security Number	Used as a unique employee identifier	N/A
Employee ID	Used to identify employee.	N/A
Name	Used to identify the employee	N/A
Work Email Address	Used for communication	N/A
Personal Mailing Address	Used for communication.	N/A
Personal Phone Number(s)	Used for communication	N/A
Personal Email Address	Used for communication	N/A
Emergency Contact Information	Used to identify the first person/s to contact in case of a medical or other crisis.	
Medications	Used to reference and document employee medications	
Medical Records	Used to document employee medical information and make medical determinations	

Gender	Used to identify employee gender	N/A
Date of Birth	Used to identify employee age and confirm identity	N/A
Race/Ethnicity	Voluntarily self-reported for employee HR record feed into eSHORE medical record as demographic data	N/A
Medical Record Number	Used for identification of employee medical record	N/A
Job Position	Used to identify employee position and occupational requirements	N/A

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?

The Reports module in eSHORE pulls data from the database and generates reports for analysis. Data produced from the Reports module are filtered results containing employee occupational health, safety, and compliance data.

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.

The system itself does not create or make available new or unutilized information about individuals. Users in specific security roles can generate custom reports that retrieve information from the database where information is stored.

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 at rest is encrypted with AES-256. AWS Key Management System (KMS) is used for keys.

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

Social security numbers in transit are encrypted with TLS 1.2/1.3. Social Security numbers at rest are protected with AES-256. The Social Security Number shown in the application will be truncated to show the last four numbers only. Social Security Numbers will only be available to personnel with a need to know. Multifactor authentication is required for users to access the system and user must be on the VA network to access the system.

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

eSHORE employs AES-256 for data at rest. Data in transit is protected using HTTPS to secure the traffic. 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?

eSHORE follows the need-to-know principle of only granting access to the data users need to perform the functions of their official duties. eSHORE users are put into security roles based on job position that determines level of access to PII. The default security role, "employee",

assigned to personnel only provides access to their 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?

eSHORE 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 eSHORE 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 eSHORE training if assigned a role other than Employee. Personnel must successfully attain a Public Trust clearance.

2.4c Does access require manager approval?

Default access is established when HR-Feed synchronizes with eSHORE to create a chart, which automatically creates a user account(s) after chart creation. eSHORE users must have a VA network account for user(s) to login with single sign-on. VA users accessing eSHORE 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. Auditing of eSHORE is at the click level for each user.

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 security 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*

PII/PHI that is retained is Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Medications, Medical Records, Race/Ethnicity, Medical Record Number, Gender, Work Email Address, Employee ID, and Job Position.

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.*

eSHORE is a cloud hosted application following the Department of Veterans Affairs Records Control Schedule (RCS) 10-1 and General Records Schedule (GRS) 2.7. Information retention length is listed below:

a. **Item Number 3015.1, Clinic Scheduling Records**
   Temporary. Destroy when 3 years old, but longer retention is authorized if needed for business use.

b. **Item Number 3015.6, Occupational individual Medical Case Files**
   a. **Long-term records**- Temporary. Destroy 30 years after employee separation or when the Official Personnel Folder (OPF) is destroyed, whichever is longer.
   b. **Short-term records**- Temporary. Destroy 1 year after employee separation or transfer.
   c. **Individual employee health case files created prior to establishment of the Employee Medical File system in 1986**- Temporary. Destroy 60 years after retirement to the NARA records storage facility.

c. **Item Number 3015.7, Non-Occupational individual Medical Case Files**
   Temporary. Destroy 10 years after the most recent encounter, but longer retention is authorized if needed for business use.

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, all records stored within eSHORE are on an approved disposition authority listed under Department of Veterans Affairs Records Control Schedule (RCS) 10-1 and NARA General Records Schedule (GRS) 2.7.

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

a. DAA-GRS 2017-0010 0001, Item Number 3015.1, Clinic Scheduling Records
b. DAA-GRS 2017-0010 0009, Item Number 3015.6, Occupational individual Medical Case Files
c. DAA-GRS-2017-0010-0012, Item Number 3015.7, Non-Occupational Individual Medical Case Files

The records retention schedule for VHA is RCS 10-1 or General Records Schedule (GRS) 2.7 at:
http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf
grs02-7.pdf (archives.gov)

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.

At the end of a record's mandatory retention period the following destruction, elimination, or transfer methods will be taken.

1. The Employee Medical File (EMF) is maintained for the period of the employee's service in the agency and is then transferred to the National Personnel Records Center (NPRC) for storage, or as appropriate, to the next employing Federal agency. Other medical records are either retained at the agency for various lengths of time in accordance with the National Archives and Records Administration's records schedules or destroyed when they have served their purpose or when the employee leaves the agency. Within 90 days after the individual separates from the Federal service, the EMF is sent to the National Personnel Records Center for storage. Destruction of the EMF is in accordance with General Records Schedule-1(21).

NARA General Records Schedules 1 and 2 specify that the following Federal civilian personnel, medical, and pay records must be centrally stored at the National Personnel Records Center (NPRC) (Civilian Personnel Records) at 111 Winnebago Street in St. Louis, Missouri:

a. Medical folders of separated Federal civilian employees.

b. An SF-135, Records Transmittal and Receipt, will be prepared to transfer any of the above types of records to the NPRC.

2. Paper records from eSHORE containing PII/PHI must be destroyed by pulping, macerating, shredding, or otherwise definitively destroying information contained in the records.

3. Digital records on the eSHORE application are deleted, then permanently deleted from the deleted items, or recycle bin after meeting the mandatory retention length.

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.

eSHORE does not use real PII for research, testing or training. Mock PII data is used for research, testing, or training.

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 information in eSHORE will be retained for longer than necessary until NPRC has an electronic solution to electronically receive the EMF from the VA.

Mitigation: This risk is mitigated by implementing secure storage, access control, and data encryption for sensitive information in the EMF during its life on eSHORE systems. Per NPRC the VA will keep electronic EMF records on their system until the organization has a solution in place to receive them via digital transfer.

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 Resources – Payroll Application Services (HR-PAS)	Receive employee demographic information from HR-PAS.	Social Security Number, Name, Work Email Address, Personal Mailing Address, Gender, Date of Birth, Job Position, Employee ID, Ethnicity, Race	Data will be electronically transmitted using HTTPS
VA Microsoft Active Directory Azure Assessing (Entra ID)	Single Sign-On application to interface with eSHORE for identification and authentication of users.	Name and Email Address	Electronic Transmission-Lightweight Directory Access Protocol over Secure Socket Layer (SSL)(LDAPS), Security

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*
			Assertion Markup Language (SAML), HTTPS

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: There is a risk that information will be shared with an unauthorized VA program for purposes other than the purpose for which it was collected.

Mitigation: Safeguards are implemented to ensure data is not sent to an unauthorized VA program, to include employee security and privacy training, and required reporting of suspicious activity. Encryption is utilized during information transmission. A Data Sharing Agreement between HR-PAS and eSHORE defines the sharing of information scope and security requirements.

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				

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: eSHORE does not share data externally.

Mitigation: eSHORE does not share data externally.
Privacy policies are posted at EOH facilities.

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.

This Privacy Impact Assessment (PIA) 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 also provided in the Federal Register with the publication of the SORN:

08VA05 / 88 FR 4885, Employee Medical File System Records (Title 38)-VA

OPM SORN GOVT-10 Employee Medical File Systems Records

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

The Federal Register publication of the eSHORE System of Record Notice (SORN) is located at the URL below:

08VA05 / 88 FR 4885, Employee Medical File System Records (Title 38)-VA and OPM SORN GOVT-10 Employee Medical File Systems Records

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.

While individuals have the right to decline providing their information, it's important to note that not providing the requested information may adversely affect the verification process or the level of service they receive.

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 in accordance with the Privacy Act and is shared with VA employees when the information is needed in accordance with job requirements or when there is authority under b(1) of the Privacy Act. In addition, individuals may consent to additional uses of the information.

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 VA employees will not know that eSHORE collects, maintains, and/or disseminates PII and other Sensitive Personal Information (SPI) about them.

Mitigation: eSHORE mitigates this risk by ensuring that it provides individuals notice of information collection and notice of the system's existence through the methods 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.***

VA Privacy Service publishes SORNs on the VA Privacy web site. SORNs contain "Notification" and "Access Procedures" detailing how individuals may request access to their information.

Separated employees requesting access to and contesting the contents of records must submit to the Human Resources Management Office at the facility where last employed with 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.

Active VA employees can gain access to the application with their VA PIV, Pin, and network account to ensure the accuracy of the information collected.

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)?

eSHORE 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?

eSHORE is a Privacy Act system.

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

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

Individuals 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.

Current VA employees identifying inaccurate or erroneous medical information, should engage EOH clinical staff assigned to respective facility to update their 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.

Individuals are notified of procedures for correcting their information through SORN ''Employee Medical File System Records (Title 38)–VA'' (08VA05) and "OPM SORN GOVT-10 Employee Medical File Systems Records".

The eSHORE Administrator, identified for each facility, can guide users to seek corrections via Human Resources (HR) for data obtained through HR feed or clinical staff for medical corrections.

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.

Redress instructions are available to the public on the VA Privacy website. Active employees will be able to manage demographic information via the eSHORE Employee Portal, some information may be overwritten with deltas imported into eSHORE from interface connection. Active employees can consult their EOH clinical staff about updates to health information. Information in eSHORE obtained from HR-PAS will require the affected user to address human resources for corrections.

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: Individuals whose records contain incorrect or out-of-date information may be exposed to the risk of not receiving proper vaccinations, notification of appointments, or test results timely. Certain incorrect information in an employee medical record could result in improper diagnosis and treatments.

Mitigation: VHA built-in procedures requires staff verify information in employee medical records and correct information identified as incorrect during each patient's medical appointments. Staff are informed of the importance of maintaining compliance with VA Request for Information policies and procedures and the importance of remaining alert to information correction requests. Individual patients have the right to request an amendment (correction) to their health information in VHA records if they believe it is incomplete, inaccurate, untimely, or unrelated to their care. The individuals must submit request in writing, specify the information that they want corrected, and provide a reason to support their request for amendment. All

amendment requests should be submitted to the facility Privacy Officer at the VHA EOH health care facility that maintains the patient's information or health records. Refer to https://www.va.gov/health/ and select "VA Privacy Practices" to view VHA Notice of Privacy Practices (NOPP) for privacy rights.

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?

VA paid employees and trainees (Employee Portal Users) receive access to the eSHORE application with an existing VA Network Account that is configured to use a smart card to login for multifactor authentication. eSHORE users have completed the VA onboarding process successfully to have a provisioned VA network account to access eSHORE. The HR-Feed will create the users record in eSHORE. Alternatively, users whose records are not created by the HR-Feed works with their eSHORE Facility Administrator to submit a request for their eSHORE user account to be manually provisioned. Users login with Single Sign On (SSO) to access their employee medical record in eSHORE. If a user's record hasn't been created the user will not be able to login. In addition, an eSHORE user must have an enabled Active Directory account to login to the eSHORE employee portal.

EOH clinician and VHA Clinical Support Staff receive access to the eSHORE application with an existing VA Network Account that is configured to use a smart card to login for multifactor authentication. eSHORE clinicians and Support Staff have completed the VA onboarding process successfully to have a provisioned VA network account to access eSHORE. EOH clinicians must complete eSHORE web-based modules followed by Virtual Instructor Led Training (VILT) prior to gaining access to the eSHORE Web Chart. VHA Clinical Support Staff must complete eSHORE web-based training prior to gaining access to the eSHORE Web Chart. Clinicians and VHA Clinical Support Staff users access the web application with Single Sign On (SSO). An HR-Feed will create the users record in eSHORE. Alternatively, users whose records are not created by the HR-Feed works with their eSHORE Facility Administrator to submit a request for their eSHORE user account to be manually provisioned. If a user's record hasn't been created the user will not be able to login. In addition, an eSHORE user must have an enabled Active Directory account to login to the eSHORE application.

eSHORE Administrators receive access to the eSHORE application with an existing VA Network Account that is configured to use a smart card to login for multifactor authentication. eSHORE Administrators have completed the VA onboarding process successfully to have a provisioned VA network account to access eSHORE. eSHORE Administrators must complete eSHORE Administrator training prior to gaining access to the eSHORE Web Chart. eSHORE users access the web application with Single Sign On (SSO). An HR-Feed will create the users record in eSHORE.

Alternatively, users whose records are not created by the HR-Feed works with their eSHORE Facility Administrator to submit a request for their eSHORE user account to be manually provisioned. If a user's record hasn't been created the user will not be able to login. In addition, an eSHORE user must have an enabled Active Directory account to login to the eSHORE application.

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?

eSHORE 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.

The available roles are:

- **Administrative Assistant**- View and access EOH patient data in assigned facility, schedule appointments, run reports, limited view access to users in facility. Aligns with business user persona EOH Support Staff.

- **Clinical Staff**- Has the ability to document encounters, immunizations, disease immunity, and protection. Order labs, x-rays, and audiology test. Schedule appointments and follow-ups. Visibility is limited to the user's facility. Has the ability to search and view data of facilities, view and run reports and dashboards. Has access to standardized reporting within their VISN. Aligns with business user persona EOH Nurse, Provider, VISN User.

- **Employees**- Has access to submit self-reported immunizations, declinations, exemption, schedule appointments, update medications, and other medical or demographic information for themselves. Aligns with business user persona EOH Patients (Employee Portal User).

- **Facility Admin**- Can edit, add, and delete all users. Aligns with business user persona eSHORE Facility Administrator.

- **SuperUser–**Has system administrator permissions with the ability to configure, deploy, and view all information in the system. Can edit, add, and delete all users. This role is being used by the implementation team and in the future, will be used by the sustainment team.

- **System Owner**- Has the ability to create reports, export reports, update user security roles, view data from all facilities, manage legal holds, and manage user provisioning and deactivation. Has system administrator permissions with the ability to configure, deploy, and view all information in the system. Can edit, add, and delete all users. Aligns with business user persona EOH VHA CO User and eSHORE System Administrator.

- **VHA Non-EOH Support Staff**- Has access to view and log immunizations administered or act as a scribe. Aligns with business user persona VHA Non-EOH Support Staff.

- **View Only**- Has the ability to view all system information and run reports. Aligns with business user persona View Only User.

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.

Yes, the VA contractor team supports the eSHORE production and preproduction environments and has access to the system and data contained therein. A contractor BAA has been developed for the system. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security Awareness and Rules of Behavior and HIPAA training via the VA's Talent Management System (TMS). The contractor personnel will be appropriately cleared and qualified under the provisions of VA policy and access to the system authorized by the appropriate personnel. The eSHORE team will update the application, operating system, introduce new functionality, govern deployment activities, and ensure user operability.

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 authorized users of VA Information Systems will receive initial VA Privacy and Information Security Awareness and Rules of Behavior (WBT) and Privacy and HIPAA training as a condition of access and, thereafter, complete the training annually. Privileged users are required to complete Information Security and Privacy Role-Based Training for System Administrators.

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

No.

8.4a If Yes, provide:

1. *The Security Plan Status:* In draft form
2. *The System Security Plan Status Date:* In draft form
3. *The Authorization Status:* Not yet authorized
4. *The Authorization Date:* Not yet authorized
5. *The Authorization Termination Date:* Not yet authorized
6. *The Risk Review Completion Date:* Not yet authorized
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.***
2/20/2025

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)*

Yes, eSHORE uses cloud technologies in Veterans Affairs Enterprise Cloud (VAEC) hosted in AWS GovCloud High which has a FedRAMP provisional authorization. eSHORE will use the IaaS and PaaS service models in the VAEC.

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.*

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.

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.

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).

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 provided in this Privacy Impact Assessment is true and accurate.

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2024.09.04 15:00:17 -04'00'

Privacy Officer, Nancy Katz-Johnson

ROBERT GAYLOR
2024.08.26 13:29:31
-06'00'

Information Systems Security Officer, Robert Gaylor

AARON DREW

Digitally signed by AARON DREW
Date: 2024.08.27 10:02:55 -04'00'

Information Systems Owner, Dr. Aaron Drew

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).

eSHORE Applicable SORN's:

08VA05 / 88 FR 4885, Employee Medical File System Records (Title 38)-VA and OPM SORN GOVT-10 Employee Medical File Systems Records

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