Privacy Impact Assessment for the VA IT System called:

Standards and Commercial off-the-shelf (COTS) Integration Platform (SCIP) Veterans Affairs Enterprise Cloud (VAEC)

VA Office of Information and Technology (OI&T) Information Technology Operations and Services (ITO)

Veterans Health Administration (VHA)

Date PIA submitted for review:

7/7/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	Dino Bonifacio	Dino.Bonifacio@va.gov	737-224-1034
Information System Owner	Andrew Carter	Andrew.Carter@va.gov	765-593-9034

Abstract

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

The Standards and Commercial Off-The-Shelf (COTS) Integration Platform (SCIP) Veterans Affairs Enterprise Cloud (VAEC) system supports the exchange of electronic health information between the Department of Defense (DoD) and the Department of Veterans Affairs (VA). This provides VA clinicians real-time access to DoD health information for patients being treated at VA facilities. The provision of DoD electronic health information to VA clinicians supports the goals of Presidential Review Directive #5, August 1998 to improve cooperation and coordination between DoD and VA to maintain the health of military personnel, Veterans, and their families as well as to address health preparedness for Veterans and their families after missions. This system also supports the goals of the VA Electronic Health Record Modernization (EHRM) effort to support interoperability with DoD by enabling the seamless sharing of records from active duty and providing Veterans and clinicians with a complete picture of patients' medical history.

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. The IT system name and the name of the program office that owns the IT system.

The Standards and COTS Integration Platform (SCIP) is a system owned by the Department of Veterans Affairs (VA) IT Operations and Services (ITOPS) Office of Information and Technology (OIT) Solution Delivery (SD) program office.

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

SCIP VAEC provides secure, bidirectional, real-time interagency exchange of clinical data between Department of Veterans Affairs (VA) and Department of Defense (DoD) health information systems. The SCIP VAEC system is comprised of several components including the Acuo Node, Central VistA Imaging Exchange (CVIX), Cerner-CVIX Integration Adaptor (CCIA), Legacy Viewer Sustainment (LVS), and Station 200 (STA200). The Acuo Node provides clinical imaging documentation from the DoD Enterprise Clinical Image Archive (ECIA) to CVIX. CVIX functions as a specialized VistA Imaging Exchange (VIX) for DoD and VA clinical users that provides these users image data from VA facilities for shared patients and DoD image data for shared patients through VistA at Station 200 (STA200). CCIA extends the capabilities of CVIX to facilitate integration with the Cerner Electronic Health Record (EHR)/ CareAwareMultiMedia (CAMM) platform. LVS supports the transfer of clinical information from the DoD Data Exchange Services (DES) to the VA's Computerized Patient Record Service (CPRS) Remote Data Views (RDV) via the VA Data Access Service (DAS). Station 200 supports the communications between LVS and CPRS RDV. By facilitating the provision of health information to VA clinicians for the purposes of healthcare, these components support the mission of VA OIT to collaborate with business partners to create the best experience for all Veterans, as well as the mission of VA to serve the men and women who are America's Veterans.

C. Indicate the ownership or control of the IT system or project.

The system is VA-owned.

2. Information Collection and Sharing

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

The system is not expected to store any information on individuals but rather to serve as a pass-through system facilitating health information sharing between other systems.

E. A general description of the information in the IT system and the purpose for collecting this information.

The system does not collect any information on individuals but rather serves as a pass-through system facilitating health information sharing between other systems.

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

VistA users can initiate requests from VistA Imaging (Image Viewer, VistA Imaging Clinical Display, VistA Rad, etc.) for clinical image information. These requests are sent to the VistA Image Exchange (VIX) containing a set of query parameters for the requested health information including the patient ID and the specific data being requested. VIX then sends this request to CVIX, which retrieves data from remote image sources including DoD leveraging DoD Electronic Data Interchange Personal Identifier (EDI-PI) to CVIX. For DoD data, CVIX then sends a request to the SCIP VAEC Acuo Node containing a set of query parameters for the image data to be retrieved along with the patient's DoD EDI-PI. SCIPVAEC Acuo Node retrieves the requested Digital Imaging and Communications in Medicine (DICOM) images from the DoD ECIA and transmits them back to CVIX, which processes and transmits the information to VIX. VIX then sends a response back to the

legacy viewers with the requested health information. VistA users can initiate requests from the VistA legacy viewers (CPRS/RDV and VistA Web) for patient health information. These requests are sent to Station 200 (STA200) containing a set of query parameters for the requested health information including the patient ID and the specific data being requested. STA200 then sends a request to LVS containing filter values as Uniform Resource Locator (URL) query parameters received from the legacy viewers. LVS then sends the VA Integration Control Number (ICN) to the VA Master Patient Index (MPI) in a standard ID (PRPA_IN201309UV02) request. The VA MPI returns the patient's DoD Electronic Data Interchange Personal Identifier (EDI-PI) to LVS. LVS then sends a request to the VA Data Access Service (DAS) containing a set of query parameters for the health information to be retrieved along with the patient's DoD EDI-PI. VA DAS retrieves this information from DoD DMIX DES and transmits it back to LVS, which processes and transmits the information to STA200. STA200 then sends a response back to the legacy viewers with the requested health information.

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

The system is operated in multiple availability zones to support system availability. All availability zones are configured with the same controls to provide the same level of security.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

The citation of legal authority to operate the SCIP VAEC system was DoD through a Data Use Agreement (DUA) and further supported via Presidential Review Directive #5, August 1998. This directive identified a national obligation to address the health preparedness and readjustment of Veterans and their families after deployments as well as the need to improve cooperation and coordination between DoD, VA, and the Department of Health and Human Services (HHS), such as the sharing of health information, to maintain the health of military personnel, Veterans, and their families. System of Records (SOR) 24VA10A7 "Patient Medical Records-VA" addresses the proper use of patient health information and may be viewed at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf SOR 79VA10 "Veterans Health Information Systems and Technology Architecture (VistA) Records-VA" addresses the proper use of information related to the VistA system and may be viewed at https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

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?

Both SORN were previously updated to reflect electronic records being located at VA Enterprise Cloud Data Centers/Amazon Web Services.

D. System Changes

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

No, completion of this PIA will not result in circumstances that require changes to business processes.

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

No, completion of 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.

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*
- ☐ 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)

System components request, receive, and transmit clinical imaging documentation that is primarily comprised of DICOM images but may also include the information noted above, as well as patients' DoD Electronic Data Interchange Personal Identifier (EDI-PI), Radiology Number (RAD), Consult Number (CON), Study Number, Reason for Image, and Type of Study.

PII Mapping of Components (Servers/Database)

SCIP VAEC consists of **3** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **SCIP VAEC** 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
mssqlserver	Yes	No	Clinical image documentation, which may include Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Health Insurance Beneficiary	The system requests, receives, and transmits health information electronically for use in patient healthcare.	Access to the system is limited to authorized privileged system administrators via multifactor authentication.

			Numbers Account, Internet Protocol (IP), Current Medications, Previous Medical Records, Race/Ethnicity, Tax Identification Number, Medical Record Number, Gender, Integration Control Number (ICN), Military History/Service Connection, Next of Kin, Other Unique Identifying Number (EDI-PI)		
va, cross, logging, dod1, dod2	Yes	No	Names, Social Security Numbers, date of birth, personal mailing addresses, personal phone numbers, emergency contact information, current medications, previous medical records, medical record number	The system requests, receives, and transmits health information electronically for use in patient healthcare.	Access to the system is limited to authorized privileged system administrators via multifactor authentication.

SQLEXPRESS	Yes	No	Clinical image documentation, which may include Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Health Insurance Beneficiary Numbers Account, Internet Protocol (IP), Current Medications, Previous Medical Records, Race/Ethnicity, Tax Identification Number, Medical Record Number, Gender, Integration Control Number (ICN), Military History/Service Connection, Next of Kin, Other Unique Identifying	The system requests, receives, and transmits health information electronically for use in patient healthcare.	Access to the system is limited to authorized privileged system administrators via multifactor authentication.

			Number (EDI-PI)		

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?

SCIP VAEC requests, receives, and transmits health information provided electronically by VA and DoD systems (Cerner, DoD ECIA, VistA, and VistA Imaging).

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.

Information from other health systems is required to support the provision of healthcare services. The information the system transmits facilitates clinical care and interoperability between VA and DoD by enabling seamless exchange of medical image data and artifacts. The systems providing this information are responsible for its collection while SCIP VAEC is responsible for its transmission.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

The system does not create information.

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?

SCIP VAEC requests, receives, and transmits health information provided electronically by VA and DoD systems (Cerner, DoD ECIA, VistA, and VistA Imaging).

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

Not applicable to this system.

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.

SCIP VAEC components use encryption for health information to ensure data corruption has not occurred during transmission.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

Not applicable for this system.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

The citation of legal authority to operate was DoD through a Data Use Agreement (DUA) and the Presidential Review Directive #5, August 1998. System of Records (SOR) 24VA10A7 "Patient Medical Records-VA" addresses the proper use of patient health information and may be viewed at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf SOR 79VA10 "Veterans Health Information Systems and Technology Architecture (VistA) Records-VA" addresses the proper use of information related to the VistA system and may be viewed at https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: SCIP VAEC components do not directly collect information from individuals but rather transmits information between systems. The use of health information by the SCIP VAEC system supports the missions of both VA and DoD and is directly relevant and necessary in supporting clinical care for patients. There is a risk that information transmitted may not be accurate, complete, or current.

Mitigation: The individual systems providing information to SCIP VAEC are responsible for its collection and assurance of accuracy, completeness, and timeliness. These systems have implemented security controls to support the assurance of accuracy, completeness, and recency of collected information. Transmission of health information is encrypted to protect against data corruption during transmission to ensure provided data is accurate and complete. Patient health information is correlated to unique identifiers associating patients with their corresponding health information to ensure accuracy.

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.

The SCIP VAEC system does not collect or maintain any information. SCIP VAEC components facilitate the secure electronic exchange of patient health information to provide authorized VA users access to DoD health information via secure channels. The information transmitted by the system is used to support and improve health information sharing and coordinated decision-making between VA and DoD clinicians. The following information may be included as part of transmitted patient health information and used by clinicians in support of the provision of patient healthcare: Name is used to verify patient identity. Social Security Number is used to verify patient identity. Date of Birth is used to verify patient identity and age. Mother's Maiden Name is used to verify patient identity. Personal Mailing Address is used to contact and communicate information to patients. Personal Phone Number(s) is used to contact and communicate information to patients. Personal Email Address is used to contact and communicate information to patients. Emergency Contact Information is used to contact an individual designated by the patient in the event of an emergency. Health Insurance Beneficiary Numbers are used to communicate with and bill third party healthcare plans. Internet Protocol (IP) Address Numbers are used to identify system assets. Medications are used for continuity of clinical care. Medical Records are used for continuity of clinical care. Race/Ethnicity is used for patient demographic information. Medical Record Number is used to uniquely identify patients. Gender is used for patient demographic information. Integrated Control Number (ICN) is used to verify patient identity. Military History/Service Connection is used for patient demographic information. Next of Kin is used to identify the personal representative for a patient in the event of passing. Other Data Elements are used to uniquely identify patients and are associated with patient records. here

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.

SCIP VAEC is a pass-through system and as such does not create new information about individuals. All information SCIP VAEC transmits already exists within the systems providing the information.

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.

SCIP VAEC components function as a service to facilitate secure communications between connected DoD and VA systems, enabling authorized users to access existing health records

including clinical image documentation. Clinicians may use shared information about patients in support of clinical healthcare.

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 within the information system is secured in accordance with applicable federal and VA policies for information security. Access to system resources is limited to authorized users via multifactor authentication. Authorized users are screened prior to receiving system access. Users receive annual security awareness and privacy training to maintain readiness for potential security incidents. Hosts are located behind a managed firewall on a secure subnet. Network traffic is monitored and audited. System interconnections are limited to authorized connections.

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

Access to the system is limited to authorized privileged system administrators via multifactor authentication.

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

The system implements appropriate administrative, technical and physical safeguards to protect the security and confidentiality of records in accordance with its assigned security categorization and security control baseline conducted in compliance with Federal Information Security Management Act (FISMA) policies. Access to system resources is limited to authorized users via multifactor authentication. Authorized users are screened prior to receiving system access. Users receive annual security awareness and privacy training to maintain readiness for potential security incidents. Hosts are located behind a managed firewall on a secure subnet. Network traffic is monitored and audited. System interconnections are limited to authorized connections. The VAEC environments all have a U.S. Federal Risk and Authorization Management Program (FedRAMP) High Certified VA Authority to Operate (ATO), which encompasses physical and environmental security including facility access authorizations and control.

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?

Access to the system is limited to authorized VA personnel for compelling operational needs. All personnel authorized to access the system must take VA-mandated security and privacy training.

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

Access control procedures for the system are documented as part of the system security plan.

2.4c Does access require manager approval?

Access to the system requires the approval of the system owner.

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

Access control procedures for the system are documented as part of the system security plan. System access is monitored and audited.

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

Local system staff are responsible for assuring safeguards are implemented for data within the system boundary.

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

As a pass-through system, the system does not retain the information identified in question 1.1.

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.*

Information is only temporarily on the system for no more than 30 days for the purpose of completing requests and is removed from the system once the information is no longer needed to complete the request.

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.
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?

As a pass-through system, the system does not store records.

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

The system follows the guidelines established in the VA and NARA-approved Department of Veterans' Affairs Record Control Schedule (RCS)10-1 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf) for Output in Electronic Form. Information is only temporarily on the system for no more than 30 days for the purpose of completing requests and is removed from the system once the information is no longer needed to complete the request.

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.

Information is only temporarily on the system for no more than 30 days for the purpose of completing requests and is removed from the system once the information is no longer needed to complete the request. This is completed via automated electronic deletion.

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.

The system does not use PII for research, testing, or training.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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:

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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: SCIP VAEC is a pass-through system. As such, the system does not retain SPI. Sensitive data is only used for as long as necessary to fulfill the stated purpose of transmitting health information to authorized systems in support of the provision of health services. There is a very low risk that information could remain in the system for longer than 30 days due to a misconfiguration of automated electronic deletion.

Mitigation: Access to the SCIP VAEC system is limited to authorized VA personnel. All personnel authorized to access SCIP VAEC must take VA-mandated annual security and privacy training. Access control procedures for the SCIP VAEC system are documented as part of the system security plan. SPI is removed from the system once a request has been processed and is no longer necessary. System resources are monitored including for high disk usage, which would quickly identify any errors resulting from misconfiguration of automated electronic deletion.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Health Administration VistA	VistA is the current Electronic Health Record for VA, and as such contains the data required for use in patient healthcare. Clinical images are shared to facilitate the provision of healthcare services to shared VA and DoD patients.	Clinical image documentation, which may include Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Health Insurance Beneficiary Numbers Account, Internet Protocol (IP), Current Medications, Previous Medical Records, Race/Ethnicity, Tax Identification Number, Medical Record Number, Gender, Integration Control Number (ICN), Military History/Service Connection, Next of Kin, Other Unique Identifying Number (EDI-PI)	Electronic (DICOM, FHIR metadata, RESTful services)
Veterans Health Administration VistA CPRS	CPRS facilitates the exchange of data with VistA.	Query parameters for clinical information containing the patient ID (VA Integration Control Number (ICN)) and the type of clinical data being requested such as Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc.), service information, medical information, and benefit information	Electronically sent via a CPRS RDV remote procedure call to STA200 and returned via an RDV response
Veterans Health Administration VistA Imaging	Clinical images are shared to facilitate the	Clinical image documentation, which may include Name, Social	Electronic (DICOM, FHIR metadata, RESTful services)

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*
	provision of healthcare services to shared VA and DoD patients.	Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Health Insurance Beneficiary Numbers Account, Internet Protocol (IP), Current Medications, Previous Medical Records, Race/Ethnicity, Tax Identification Number, Medical Record Number, Gender, Integration Control Number (ICN), Military History/Service Connection, Next of Kin, Other Unique Identifying Number (EDI-PI)	
Veterans Health Administration Master Person Index (MPI)	This system correlates the patient's Integrated Control Number (ICN) with the patient's EDI-PI.	Integration Control Number (ICN), Electronic Data Interchange-Personal Identifier (EDI-PI), and other parameters necessary to gather DoD data from the Data Exchange Service (DES) for the requested type of clinical data	Electronic Health Level 7 (HL7) v3 service sends standard ID (PRPA_IN201309UV02) request
Data Access Service Data Access Service (DAS)	The information received and shared with this system is for use in patient healthcare. Specifically, this system requests and retrieves patient information	Clinical image documentation, which may include Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Health Insurance Beneficiary	Electronic (DICOM, FHIR metadata, RESTful services)

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*
	from the DoD DES system and facilitates the exchange of clinical images with DoD for the provision of healthcare services.	Numbers Account, Internet Protocol (IP), Current Medications, Previous Medical Records, Race/Ethnicity, Tax Identification Number, Medical Record Number, Gender, Integration Control Number (ICN), Military History/Service Connection, Next of Kin, Other Unique Identifying Number (EDI-PI)	

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: Due to the nature of the information shared, the internal sharing of health information presents a risk of harm to the organization and individuals whose information is exchanged if an unauthorized individual were to access this information.

Mitigation: Access to SCIP VAEC is limited to authorized personnel. The SCIP system employs technical safeguards against unauthorized access based on NIST SP 800-53 and enforces management, operational and technical controls to protect information processed and transmitted by the system.

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***

Department of Defense (DoD) Cerner	Clinical images are shared to facilitate the provision of healthcare services to shared VA and DoD patients.	Clinical image documentation, which may include Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Health Insurance Beneficiary Numbers Account, Internet Protocol (IP), Current Medications, Previous Medical Records, Race/Ethnicity, Tax Identification Number, Medical Record Number, Gender, Integration Control Number (ICN), Military History/Service Connection, Next of Kin, Other Unique Identifying Number (EDI-PI)	Presidential Review Directive #5, August 1998; System of Records (SOR) 24VA10A7 "Patient Medical Records-VA"	Electronic (DICOM, FHIR metadata)
Department of Defense (DoD) ECIA	Clinical images are shared to facilitate the provision of healthcare services to shared VA and DoD patients.	Clinical image documentation, which may include Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Health Insurance Beneficiary Numbers Account, Internet Protocol (IP), Current Medications, Previous Medical Records, Race/Ethnicity, Tax Identification Number, Medical Record Number, Gender, Integration Control Number (ICN), Military History/Service Connection, Next of Kin, Other Unique Identifying Number (EDI-PI)	Presidential Review Directive #5, August 1998; System of Records (SOR) 24VA10A7 "Patient Medical Records-VA"	Electronic (DICOM, FHIR metadata)
Defense Health Agency Date Exchange Service (DES)	Health data is shared to facilitate the provision of healthcare	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Health Insurance Beneficiary Numbers Account,	Presidential Review Directive #5, August 1998; System of Records	

	services to shared VA and DoD patients.	Internet Protocol (IP), Current Medications, Previous Medical Records, Race/Ethnicity, Tax Identification Number, Medical Record Number, Gender, Integration Control Number (ICN), Military History/Service Connection, Next of Kin, Other Unique Identifying Number (EDI-PI)	(SOR) 24VA10A 7 "Patient Medical Records-VA"	
Defense Health Agency SADR (Standard Ambulatory Data Record) CAPER (Comprehensive Ambulatory/Professio nal Encounter Record) and PDTS (Pharmacy Data Transaction Service)	Health data is shared to facilitate the provision of healthcare services to shared VA and DoD patients.	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Health Insurance Beneficiary Numbers Account, Internet Protocol (IP), Current Medications, Previous Medical Records, Race/Ethnicity, Tax Identification Number, Medical Record Number, Gender, Integration Control Number (ICN), Military History/Service Connection, Next of Kin, Other Unique Identifying Number (EDI-PI)	Presidenti al Review Directive #5, August 1998; System of Records (SOR) 24VA10A 7 "Patient Medical Records-VA"	Secure FTP

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: Unauthorized disclosure of PHI/PII/SPI, whether intentional or unintentional, could have an adverse impact on VA and affected patients.

Mitigation: Access to the SCIP VAEC system is limited to authorized VA personnel. All personnel authorized to access SCIP VAEC must take VA-mandated annual security and privacy training. Remote access to the system is only allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. Audit logs are collected and reviewed. Technical and physical controls are documented as part of the system security plan. SPI is removed from the system once a request has been processed.

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.

SCIP VAEC is a pass-through system which does not directly collect information from individuals. The system exchanges information electronically on behalf of other systems. Notice for the collection of information from individuals is the responsibility of the systems collecting and providing information to SCIP VAEC. 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. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non-Veterans receiving care are provided the notice at the time of their encounter. This Privacy Impact Assessment (PIA) also serves as notice as required by the eGovernment Act of 2002, Pub. L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority, and the conditions under which the information can be disclosed. Notice is also provided in the Federal Register with the publication of these SORNs:24VA10A7 "Patient Medical Records-VA" may be viewed at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for

maintenance of the system: Title 38, United Stats Code, Section 501(b) and 304.SORN 79VA10 "Veterans Health Information Systems and Technology Architecture (VistA) Records-VA" may be viewed at https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. Authority for maintenance of the system: Title 38, United States Code, section 7301(a).

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

SCIP VAEC is a pass-through system which does not directly collect information from individuals. Notice for the collection of information from individuals is the responsibility of the systems connecting to SCIP VAEC.

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.

SCIP VAEC is a pass-through system which does not directly collect information from individuals. The system exchanges information electronically on behalf of other systems. Notice for the collection of information from individuals is the responsibility of the systems collecting and providing information to SCIP VAEC. Several notices of usage are described above.

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.

SCIP VAEC is a pass-through system which does not directly collect information from individuals. The opportunity and right to decline the provision of information is managed by the systems connecting to SCIP VAEC. Individuals seeking information regarding access to and contesting of VA records may contact the Privacy Officer at the nearest VA Medical Center.

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.

SCIP VAEC is a pass-through system which uses health information in support of patient health services. Notice for the collection of information from individuals is the responsibility of the systems connecting to SCIP VAEC. Information is used, accessed, and disclosed in accordance with the

Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR. Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed, and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR. Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

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 individuals may not be aware their information is being received or transmitted by the system.

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

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.***

SCIP VAEC is a pass-through system which does not store or retain information on individuals. All information the system transmits is stored, retained, and managed by the systems providing information to SCIP VAEC. Procedures and regulations for individuals accessing their information are specific to these systems There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office. VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access.VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records. Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact Contract Officer Representative (COR) to obtain information upon request.

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).

The Privacy Act covers systems that store individual records to establish policies and procedures under which a subject individual may be given notification of or access to a pertinent record. SCIP VAEC is a pass-through system which does not store or retain records on individuals but transmits information between other information systems for the purpose of use in patient care. Procedures and regulations for individuals to gain access to their records are specific to those systems.

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.

The Privacy Act covers systems that store individual records to establish policies and procedures under which a subject individual may be given notification of or access to a pertinent record. SCIP VAEC is a pass-through system which does not store or retain records on individuals but transmits information between other information systems for the purpose of use in patient care. Procedures and regulations for individuals to access their records are specific to those systems.

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.

SCIP VAEC is a pass-through system which does not store or retain any information on individuals. All information the system transmits is stored, retained, and managed by the systems providing information to SCIP VAEC. Procedures for correcting inaccurate or erroneous information are provided by these systems. Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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.

SCIP VAEC is a pass-through system which does not store or retain any information on individuals. All information the system transmits is stored, retained, and managed by the systems providing information to SCIP VAEC. Notification for procedures for correcting inaccurate or erroneous information are provided by these systems. Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) which states: Right to Request Amendment of Health Information. You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following: file an appeal; file a "Statement of Disagreement"; or ask that your initial request for amendment accompany all future disclosures of the disputed health information. Individuals seeking information

regarding access to and contesting of VA benefits records may write, call or visit the nearest VA regional office. Additional notice is provided through the SORS listed in 6.1 of this PIA and through the Release of Information Office where care is received.

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.

SCIP VAEC is a pass-through system which does not store or retain any information on individuals. All information the system transmits is stored, retained, and managed by the systems providing information to SCIP VAEC. Formal redress and/or alternatives are provided by these systems.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

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

Mitigation: SCIP VAEC is a pass-through system which does not store or retain any information on individuals. All information the system transmits is stored, retained, and managed by the systems providing information to SCIP. The risk of incorrect information in an individual's records is mitigated by authenticating information when possible. The NOPP discusses the process for requesting an amendment to one's records. Individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office.

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.

Access to SCIP VAEC is limited to VA contractor personnel directly involved in the maintenance and support of the system and cleared administrative staff whose duties require access.

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?

Not applicable to this system as there are no external users from other agencies.

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.

Access is limited to privileged system administrators.

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.

Access to SCIP VAEC is limited to VA contractor personnel directly involved in the maintenance and support of the system and cleared administrative staff whose duties require access. Contractors

who work on the system sign the standard VA Information Protection and Risk Management Non-Disclosure Agreement (NDA) prior to gaining access to any VA information under the contract. Contractors also sign the VA Rules of Behavior on an annual basis as part of their security awareness training. Contractors who support the SCIP system are required to have a Public Trust. Access to PII within the system is necessary for system administrators and database administrators to perform essential operations and maintenance tasks as privileged system users.

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.

Access to SCIP VAEC is limited to personnel directly involved in the operations and maintenance of the system as well as cleared administrative personnel whose duties require access. These personnel are required to take privacy and security training provided by VA in accordance with all relevant VA training requirements. As SCIP VAEC does not provide any other users with access to PII, there is no separate privacy or security training specific to the system.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* May 10, 2022
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* September 15, 2022
5. *The Authorization Termination Date:* September 15, 2025
6. *The Risk Review Completion Date:* July 28, 2022
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.***

Not applicable for this system.

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, the SCIP VAEC system is hosted within Amazon Web Services (AWS) GovCloud East as part of VAEC under the Infrastructure as a Service (IaaS) model. There is an agreement in place between AWS and VA under VAEC-Amazon Web Services (VAEC-AWS): Enterprise Cloud Capacity Contract – NNG15SD22B VA118-17-F-2284. The Cloud Service Provider (CSP), AWS, was assessed under FedRAMP. Security controls are tested as part of the authorization process for the FedRAMP High Baseline and DoD Impact Level 4 by a third-party assessment organization (3PAO).

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.*

Please provide response here

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.

Please provide response here

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.

Please provide response here

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).

Please provide response here

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Phillip Cauthers 255139

Digitally signed by Phillip Cauthers 255139
Date: 2023.07.20 08:28:43 -07'00'

Privacy Officer, Phillip Cauthers

DINO BONIFACIO

Digitally signed by DINO BONIFACIO
Date: 2023.07.21 06:49:07 -05'00'

Information System Security Officer, Dino Bonifacio

ANDREW CARTER

Digitally signed by ANDREW CARTER
Date: 2023.07.21 09:36:40 -04'00'

Information System Owner, Andrew Carter

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).

The VHA Notice of Privacy Practice (NOPP) explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non-Veterans receiving care are provided the notice at the time of their encounter.
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

SORN: 24VA10A7 "Patient Medical Records-VA" may be viewed at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for maintenance of the system: Title 38, United Stats Code, Section 501(b) and 304.

SORN: 79VA10 "Veterans Health Information Systems and Technology Architecture (VistA) Records-VA" may be viewed at https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. Authority for maintenance of the system: Title 38, United States Code, section 7301(a).

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

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

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