Privacy Impact Assessment for the VA IT System called:

Joint Longitudinal Viewer-Veterans Affairs Enterprise Cloud (JLV-VAEC)

Veterans Health Administration (VHA)

Office of Health Informatics (OHI)

eMASS ID #1112

Date PIA submitted for review:

November 16, 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	Christopher Brown	Christopher.Brown1@va.gov	202-270-1432

Abstract

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

The Joint Longitudinal Viewer-Veterans Affairs Enterprise Cloud (JLV-VAEC) is a custom web presentation system that pulls information from several health care systems (in real-time) for presentation in a browser. The JLV-VAEC Web Application provides the ability to view specific clinical data stored in any electronic medical record system. Authorized users Department of Veterans Affairs and Department of Defense (VA and DOD) medical service providers can access a patient's clinical data via a web browser. JLV-VAEC provides a common data view of read-only, real-time patient information from separate and distinct electronic medical record systems.

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 system name is Joint Longitudinal Viewer-Veterans Affairs Enterprise Cloud (JLV-VAEC) and the Product Line is Health Informatics.

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

The JLV-VAEC Web Application provides the ability to view specific clinical data stored in any electronic medical record system available to the abstraction tier. Authorized Composite Health Care System (CHCS) and Veterans Health Information Systems and Technology Architecture (VistA) users (government, military, contractor personnel with active Common Access Card (CAC) and Personal Identity Verification (PIV) cards) from each site can access a patient's clinical data via a web front end via a browser from within the sites intranet. JLV-VAEC provides a common data view of read-only, real-time patient information from separate and distinct electronic medical record systems, including VistA, CHCS and Bidirectional Health Information Exchange (BHIE).

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

Christopher Brown is the Information System Owner (ISO), and Julie Schuck is the VA Program Manager. JLV-VAEC is under the Health Informatics Product Line. The VHA Business Office work with the JLV-VAEC contract team, the PM and ISO to control, manage, develop, and sustain the application.

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?

A new service has been added to JLV-VAEC. The system can store user's queries of patient data, from DHA/VA data systems, into securely stored PDF reports for up to 72 hours. There are currently no limits on the number of patient records to be temporarily stored for reports. Reports are systematically deleted/removed by the report builder service after 72 hours.

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

JLV-VAEC provides a common data view of read-only, real-time patient information from separate and distinct electronic medical record systems, including VistA, CHCS and Bidirectional Health Information Exchange (BHIE). A user has access to a provider portal, which provides information specific to the clinician, such as appointments, abnormal lab results, admissions, etc. This information is used by medical professionals to provide better and faster diagnosis of Veterans' health issues.

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

JLV-VAEC uses a data service to assemble a read-only real-time view of electronic health information from the VA Patient Medical Record.

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

JLV-VAEC is hosted at the Amazon Web Services (AWS) GovCloud VAEC. The container services listed in the Component Details tab are included for informational purposes only. These containers/services fall under the authorization boundary of the AWS GovCloud VAEC. JLV-VAEC is in the West region with multiple Availability Zones (AZ).

3. Legal Authority and SORN

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

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

SORN 24VA10A7 "Patient Medical Record – VA", Authority for Maintenance of the system: Title 38, United States Code, Section 501(b) and 304. https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf.

SORN 79VA10 "Veterans Health Information Systems and Technology Architecture (VistA)". Collection of that data and maintaining the system are authorized by Title 38,

United States Code, Section 501. (The audit log portion of this system), 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?*

The SORN does not require amendment or revision and approval. Yes, the system location in SORN 24VA10A7 specifies that data may be maintained in the VA Enterprise Cloud Data Centers/Amazon Web Services.

4. System Changes

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

No changes to business processes are required upon the completion of this PIA.

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

The 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. 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: VA Patient IEN/ICN, DoD Patient EDIPI, DoD User CAC/EDIPI, VA User ID/PIV.

PII Mapping of Components (Servers/Database)

Joint Longitudinal Viewer-Veterans Affairs Enterprise Cloud consists of **1** key component (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Joint Longitudinal Viewer-Veterans Affairs Enterprise Cloud** and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

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

Relational Database Server Managed Service (RDS MS)	Yes	Yes	User's Name, ID/PIV/CAC, Patient SSN, Workstation IP address	Used for audit logging	Amazon RDS encrypted using AES-256 algorithm

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?

There are two data sources for JLV-VAEC. At DOD there is Composite Health Care System (CHCS) and Bidirectional Health Information Exchange (BHIE), and at VA there is Veterans Health Information Systems and Technology Architecture (VistA).

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.

JLV-VAEC provides a common data view of read-only, real-time patient information from separate and distinct electronic medical record systems, including VistA, CHCS and Bidirectional Health Information Exchange (BHIE). A user has access to a provider portal, which provides information specific to the clinician, such as appointments, abnormal lab results, admissions, etc. This information is used by medical professionals to provide better and faster diagnosis of Veterans' health issues.

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

JLV-VAEC allows its users to generate reports from queries to be securely stored for up to 72 hours. This will allow users to continue with patient care while reports are being generated in the background. Audit log information is maintained for security/legal purposes.

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?

JLV-VAEC disseminates/displays information via electronic transmission from DHA and VA systems.

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?

Audit log information and report information are derived from the sources listed above.

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.

Accuracy is checked by source systems (DOD and VA VISTA) providing data feed views to JLV-VAEC.

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?

This system does not check for accuracy by accessing a commercial aggregator of information.

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

- Presidential Review Directive 5, A National Obligation – Planning for Health Preparedness for and Readjustment of the Military, Veterans, and Their Families after Future Deployments, August 1998.
- The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.
- SORN 24VA10A7 "Patient Medical Record – VA". Authority for maintenance of the system comes from Title 38, United States Code, Section501(b) and 304. https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

- The audit log portion of this system falls under, SORN 79VA10 "Veterans Health Information Systems and Technology Architecture (VistA)". Collection of that data and maintaining the system are authorized by Title 38, United States Code, Section 501. https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

- Memorandum of Understanding Between the Department of Defense (DOD) and the Department of Veterans Affairs (VA) for Sharing Personal Information, March 13, 2014.

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: JLV-VAEC disseminates a visual display of Personally Identifiable Information (PII) and other highly delicate Personal Health Information (PHI). If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The Department of Veterans Affairs is careful to only collect and secure the information necessary to accomplish the VA mission. Additionally, to identify the parties involved in an incident, identify potential issues and concerns, and aid the affected parties so that they may find the help they need to get through their crisis. By only collecting and securing the minimum necessary information, the VA can better protect the individual's information.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
JLV-VAEC disseminates/displays the following information from both internal and external sources: • SSN (Last 4 only), Veteran/Patient identification – Audit log purposes • IP address – Audit log purposes • Patient Name – Patient Identification • Patient Date of Birth – Patient Identification • Mailing Address – Contact and correspondence with patient. • Zip Code – part of the mailing address • Phone Number (s) – Contact and correspondence with patient. • Email Address - Contact and correspondence with patient. • Emergency Contact Information – Contact and correspondence with patient's next of kin.	• Audit log purposes • Patient Identification • Contact and correspondence with patient. • Contact and correspondence with patient's next of kin. • Display current health and medical conditions of the Veteran. • Historical medical history and treatment • Statistical reporting	• Audit log purposes • Patient Identification • Contact and correspondence with patient. • Contact and correspondence with patient's next of kin. • Display current health and medical conditions of the Veteran. • Historical medical history and treatment • Statistical reporting

• Current Medical Records/Medications – display current health and medical conditions of the Veteran, such as health problems, diagnoses, therapeutic procedures, X-rays, laboratory tests and surgical operations – internal/external. • Previous Medical Records – Historical medical history and treatment • Patient Race/Ethnicity – statistical reporting		
For patient treatment, JLV-VAEC temporarily, and securely, stores the following types of information for generating timely pdf-based user reports from both internal and external sources: • SSN – Last 4 only • IP address • Patient Name • Patient Date of Birth • Mailing Address • Zip Code • Phone Number(s) • Email Address • Emergency Contact Information • Current Medical Records/Medications • Previous Medical Records • Patient Race/Ethnicity – statistical reporting	• Audit log purposes • Patient Identification • Display current health and medical conditions of the Veteran. • Historical medical history and treatment • Statistical reporting	• Audit log purposes • Patient Identification • Display current health and medical conditions of the Veteran. • Historical medical history and treatment • Statistical reporting
For accountability, JLV-VAEC maintains the following data in audit logs to determine what user and/or computer accessed a specific patient's file on specific dates and times:	• Audit log purposes	• Audit log purposes

• User's Login ID/PIV/CAC • User's Name • Query Action performed. • Start/End Time/Date stamps. • Patient SSN • Workstation IP address		

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?

JLV-VAEC is a viewer that disseminates/displays electronic health information pulled from DHA and VA systems and has no ability to analyze the data it displays.

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 does not create or make available new or previously unutilized information about an individual.

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?

JLV uses encryption- TLS/HTTPS protocols to encrypt data in transit. JLV also utilizes the VA VPN for secure connections and VA firewalls to protect data in transit. For data at rest, all data is encrypted, password protected, and under-goes strict auditing and monitoring.

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

JLV does not store SSNs. JLV is a read-only application that retrieves SSN data from the Master Persons Index service.

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

JLV does not store PII/PHI data. JLV is a read-only application that displays PII/PHI data from other upstream data sources. This data is encrypted in transit and at rest. All JLV staff are required to under-go PII/PHI HIPAA training, Rules of Behavior (ROB) training and Privacy and Security (PISA) training.

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?

The System of Record Notice (SORN) defines what information can be collected from veterans, use of the information, and how the information is accessed and stored. The information collected is used for determining a veteran's benefits, such as compensation or education.

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

For the audit log portion of this system is maintained in the VISTA system under SORN 79VA10 "Veterans Health Information Systems and Technology Architecture (VistA)".

2.4c Does access require manager approval?

JLV-VAEC user access processes are described below in Section 8. Technical Access and Security.

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

The security controls for the JLV-VAEC application cover approximately 17 security areas regarding protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include access control; awareness and training; audit and accountability; certification,

accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity.

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

The JLV-VAEC application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA 6500 HB, National Rules of Behavior (ROB), and VA 6502.1, VA6502.3, VA 6502.4 Privacy Policies govern how veterans' information is used, stored, and protected.

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*

JLV-VAEC disseminates/displays the following information from both internal and external sources:

- SSN (Last 4 only), Veteran/Patient identification – Audit log purposes
- IP address – Audit log purposes
- Patient Name – Patient Identification
- Patient Date of Birth – Patient Identification
- Mailing Address – Contact and correspondence with patient.
- Zip Code – part of the mailing address
- Phone Number (s) – Contact and correspondence with patient.
- Email Address - Contact and correspondence with patient.
- Emergency Contact Information – Contact and correspondence with patient's next of kin.
- Current Medical Records/Medications – display current health and medical conditions of the Veteran, such as health problems, diagnoses, therapeutic procedures, X-rays, laboratory tests and surgical operations – internal/external.
- Previous Medical Records – Historical medical history and treatment
- Patient Race/Ethnicity – statistical reporting

For patient treatment, JLV-VAEC temporarily, and securely, stores the following types of information for generating timely pdf-based user reports from both internal and external sources:

- SSN – Last 4 only
- IP address
- Patient Name

- Patient Date of Birth
- Mailing Address
- Zip Code
- Phone Number(s)
- Email Address
- Emergency Contact Information
- Current Medical Records/Medications
- Previous Medical Records
- Patient Race/Ethnicity – statistical reporting

For accountability, JLV-VAEC maintains the following data in audit logs to determine what user and/or computer accessed a specific patient's file on specific dates and times:

- User's Login ID/PIV/CAC
- User's Name
- Query Action performed.
- Start/End Time/Date stamps.
- Patient SSN
- Workstation IP address

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.*

JLV-VAEC is able store user's queries into securely stored pdf reports for up to 72 hours. Reports are systematically deleted/removed by the report builder service after 72 hours.

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

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

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

The Record Control Schedule (RCS) 10-1 contains retention and disposition requirements for VHA records which have been authorized by NARA or have been assigned a General Record Schedule (GRS) disposal authority. The VHA RCS 10-1 is the main authority for the retention and disposition requirements of VHA records. It provides a brief description of the records, states the retention period and disposition requirements. The RCS 10-1 link is: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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

The information in JLV VAEC are retained under RCS 10-1 item 6000.2 c and may be destroyed when no longer needed for administrative or clinical operations. Disposition authority: N1-15-02-3 item 4.

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.

Audit logs and/or reports containing VA sensitive information pertaining to the system (described in section 3.1) such as IP addresses and other operational data will be destroyed in accordance with VA 6500.1 Handbook and any paper records will be destroyed in accordance with VA Directive 6371.

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 JLV-VAEC system does not use PII/PHI/SPI or production data for any research, testing, or development purposes.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains

information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

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

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

Follow the format below:

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

Mitigation: To mitigate the risk posed by information retention, JLV-VAEC adheres to the NARA General Records Schedule. When the retention date is reached for a record, the individuals' information is carefully disposed of by the determined method as described in General Records Schedule 20.

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***
Master Person Index (MPI) formerly Master Veteran Index (MVI)	Data is used by JLV-VAEC to display patient's medical records as well as create reports at user's request.	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity	Secure electronic transmission via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS). Storage of report uses AES-256 encryption.
VA Veterans Health Administration (VHA) VISTA EHR and Cerner EHR	Data is used by JLV-VAEC to display patient's medical records as well as create reports at user's request.	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity	Secure application VPN in SSL/TLS using FIPS 140-2 certified cryptographic mod
VA Veterans Benefit Administration (VBA) CAPRI/Claims	Data is used by JLV-VAEC to display patient's medical records as well as create reports at user's request.	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications	Secure application VPN in SSL/TLS using FIPS 140-2 certified cryptographic module

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*
		Previous Medical Records Race/Ethnicity	
Veterans Health Administration (VHA) Veterans Information Systems and Technology Architecture (VISTA)	Data is used by JLV-VAEC to display patient's medical records as well as create reports at user's request.	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient Internal Control Number (ICN)/Internal Entry Number (IEN)	Secure electronic transmission via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS). Storage of report uses AES-256 encryption.
Veterans Health Administration (VHA) Central Vista Imaging Exchange (CVIX)	Data is used by JLV-VAEC to display patient's medical records as well as create reports at user's request.	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient Internal Control Number (ICN)/Internal Entry Number (IEN) Clinical Images – to include scanned documents	Secure electronic transmission via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTP

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Follow the format below:

Privacy Risk: The privacy risk associate with disclosing Personal Identifiable Information (PII) is that sharing data within the Department of Veterans' Affairs is that the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: There are minimal to no privacy risks to the data captured in the system logs because JLV-VAEC does not share data with any internal Program Offices or IT systems. The system logs are securely maintained in an encrypted database under IO management. The only information shared internally is audit log information. Access to the audit logs is limited to only authorized personnel with under the direction from stakeholders and/or system/data owners for official legal purposes or investigations.

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) Patient Discovery Web Service (PDWS)	Data is used by JLV-VAEC to display DoD patient data for use in VA facilities by VA providers	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity	Presidential Review Directive 5 MOU between VA and DOD dated March 2014 ISA between VA and DOD dated July 2014-Title 38 and 42 U.S.C. Per 24VA10A7 -Patient Medical Records-Title 38 U.S.C.	Secure application VPN in SSL/TLS using FIPS 140-2 certified cryptographic modules
DOD Bidirectional Health Information Exchange (BHIE)	Data is used by JLV-VAEC to display patient's medical records as well as create reports at	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical	Presidential Review Directive 5 MOU between VA and DOD dated March 2014 ISA between	Secure electronic transmission via Transmission Control Protocol (TCP) /Digital Imaging and Communications in Medicine

	user's request.	Records Race/Ethnicity	VA and DOD dated July 2014- Title 38 and 42 U.S.C. Per 24VA10A7 -Patient Medical Records- Title 38 U.S.C.	(DICOM). Secure application VPN in SSL/TLS using FIPS 140-2 certified cryptographic module.

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: The privacy risk associated with disseminating PII/PHI is that sharing data outside of the Department of Veteran's Affairs could increase the risk that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by JLV-VAEC personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system.

Section 6. Notice

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

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

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

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

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in multiple ways:

- 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.

- 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: 24VA10A7 "Patient Medical Record – VA", Patient Medical Records Title 38, United States Code, Section 501(b) and 304. https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf.

- 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."

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

Notice is provided as described in question 6.1a above.

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.

VHA provides effective notice regarding collection, use, sharing, safeguarding, maintenance and disposal of PII, authority for collecting PII and the ability to access or amended PII through its Privacy Act SORNs. In addition, the VHA Notice of Privacy Practices (NOPP) provides notice on privacy practices including collection, use and disclosure of PII and PHI and privacy rights such as the ability to access and amendment.

The VHA NOPP is provided to newly enrolled Veterans at the time of enrollment and currently enrolled Veterans annually. VHA also provides notice on the authority for collecting PII and choices regarding the PII at the point of collection. VHA permits individuals to agree to the collection of their PII using paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what system of records the information will be stored.

The Privacy Act Statements on the paper and electronic forms explain whether data collection is mandatory or voluntary and explains the consequences of not providing the information when data collection is voluntary. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA NOPP and conversations with VHA employees.

VA Forms are reviewed by Veterans Health Administration Central Office (VHACO) periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. Lastly, VHA provides such notice in its PIAs which are published for public consumption.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

Information is used, accessed, and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

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

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

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records. The NOPP is also available at all VHA medical centers from the facility Privacy Officer.

The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

Section 7. Access, Redress, and Correction

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

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

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

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

Individuals are not given access to their information in JLV-VAEC. JLV-VAEC system data is for use by medical service providers only. As directed in the System of Record Notice (SORN) 24VA10A7 - Patient Medical Records, "Individuals seeking information regarding access to and contesting of VA medical records may write, call, or visit the last VA facility where medical care was provided."

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 http://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.

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 system is not exempt from the Privacy Act information may be obtained via the processes outlined in question 7.1b above.

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 system is not exempt from the Privacy Act information may be obtained via the processes outlined in question 7.1b above.

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 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.

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"
- 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.

Formal redress via the amendment process is available to all individuals, as stated in questions 7.1-7.3In

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: the risk of incorrect information in an individual's records is mitigated by authenticating information when possible. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.
The NOPP discusses the process for requesting an amendment to one's records.

The Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information. The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

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?

Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring are performed using TMS.

For access control, JLV-VAEC uses two-factor authentication. All authorized users (government, military, contractor personnel) must authenticate using an active credential, i.e., DOD CAC or VA PIV credential.

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?

VHA users must already have DHA system credentials as well as VistA credentials to use JLV-VAEC. These systems have their own respective access control process for users to follow.

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.

VBA users must already have VA network access and PIV cards but must also request JLV-VAEC access through CLIN3 processes for access. JLV-VAEC administrators create profiles based upon CLIN3 requests.

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.

Contractor access is verified through VA personnel before access is granted to any contractor. Contracts and contractor access are reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security (PISA) and Rules of Behavior (ROB) training via TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access.

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.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the ROB, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS 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:* 06/07/2023
3. *The Authorization Status:* Authority to Operate
4. *The Authorization Date:* 06/16/2023
5. *The Authorization Termination Date:* 06/16/2025
6. *The Risk Review Completion Date:* 06/15/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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

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

Authorized and Operating

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)*

JLV-VAEC uses VA Enterprise Cloud using Amazon Web Services (AWS) GovCloud as the service provider. The cloud service is FedRAMP approved. The contract number is VA-118-17-F-2284.

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

ID	Privacy Controls
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

PHILLIP CAUTHERS

Digitally signed by PHILLIP CAUTHERS
Date: 2024.02.06 08:56:15 -08'00'

Privacy Officer, Phillip Cauthers

DINO BONIFACIO

Digitally signed by DINO BONIFACIO
Date: 2024.02.06 11:51:11 -06'00'

Information System Security Officer, Dino Bonifacio

CHRISTOPHER BROWN

Digitally signed by CHRISTOPHER BROWN
Date: 2024.02.06 16:42:18 -06'00'

Information System Owner, Christopher Brown

APPENDIX A-6.1

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

VHA Notice of Privacy Practices
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

SORN 24VA10A7 "Patient Medical Record – VA
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

HELPFUL LINKS:

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

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

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

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

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