Privacy Impact Assessment for the VA IT System called:

Joint Legacy Viewer (JLV)

VA Office of Information Technology (OIT)

Date PIA submitted for review:

July 6, 2021

System Contacts:

System Contacts

Title	Name	E-mail	Phone Number
Privacy Officer (PO)	Rita Grewal	Rita.Grewal@va.gov	202-632-7861
Information System Security Officer (ISSO)	Andre Davis	Andre.Davis2@va.gov	512-326-7422
Information System Owner (ISO)	Christopher Brown	Christopher.Brown1@va.gov	202-270-1432

Abstract

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

Joint Legacy Viewer (JLV) is a joint venture between the Department of Defense and the Department of Veteran Affairs, the web application that provides authorized users (VA and DOD medical service providers) with the ability to view read-only clinical data stored (patient's medical records) in any electronic medical record systems available that belong to either the VA's Veterans Health Information Systems and Technology Architecture (VistA), DOD's Composite Health Care System (CHCS)/Armed Forces Health Longitudinal Technology Application (AHLTA), and MHS Genesis/JointHIE by Cerner.

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *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.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?*
- *Does the system use cloud technology? 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.

- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*
- *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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

Joint Legacy Viewer (JLV) is a custom Government Off-the-Shelf (GOTS) patient-centric, web presentation system that pulls information from disparate health care systems, from Defense Health Agency (DHA-DoD) and internal VA systems described below, in real-time for presentation in a browser design. The system is in the operational phase of the System Development Lifecycle (SDLC) and is currently being used by 5000 users. JLV is available to authorized users throughout the DOD and the Department of Veterans Affairs (VA). The JLV 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 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. The information is displayed in a consolidated collection of widgets for the corresponding clinical data types. The configuration and layout of widgets is unique for each user of the system. The user can add additional widgets by dragging the given widget from the toolbar at the bottom of the screen. The current interface (jMeadows) is a web service that retrieves clinical data from electronic medical record (EMR) systems, in this case VistA for VA.

Development and Test Environment (DTE) is a minor component of JLV that provides a test environment for future JLV development. DTE does not process, store, or maintain any live data and will never go into production. Since DTE is only for testing and development the customer does not require recovery for DTE. The minor component falls under JLV and inherits all security functions from the JLV application. The JLV production service/application resides within the VA VMWare farm offering, and therefore does not use cloud technology.

Joint Legacy Viewer is hosted at the Austin Information Technology Center (AITC) and the Philadelphia Information Technology Center (PITC). The servers listed in the Component Details tab are included for informational purposes only. These servers fall under the authorization boundary of the Infrastructure Operations (IO) UNIX and Windows Service Lines.

JLV uses a data service to assemble a read-only real-time view of electronic health information.
Per SORN 24VA10A7, recently updated from 24VA10P2 – Patient Medical Records Title 38, United States Code, Section 501(b) and 304.
A new service has been added to JLV. The system is able to 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.

JLV maintains a log for auditing purposes; it logs the patient identifier and the Internet Protocol (IP) address of the system from where the request to view a patient's file was initiated. For the audit log portion of this system, SORN 79VA10 is being updated by VHA privacy to include systems with that functionality. Collection of that data and maintaining the system are authorized by Title 38, United States Code, Section 501.

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.

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 Account Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☒ Current Medications
☒ Previous Medical Records
☒ Race/Ethnicity
☒ VA Patient EIN/ICN
☒ DoD Patient EDIPI

☒ DoD User CAC/EDIPI
☒ VA User ID/PIV

JLV is a read only viewer web-based application. Personal Health Information (PHI) is called from DOD's CHCS/AHLTA system and the VA's VistA health information system. JLV disseminates a read-only view of a patient's medical information.

JLV can store users' queries into securely stored pdf reports for up to 72 hours. Reports are systematically deleted/removed by the report builder service after 72 hours.

Only the social security number of the Veteran's record viewed and IP address of the user viewing the record are used for the audit logs of the system. All other data is disseminated in the read only viewer.

PII Mapping of Components

JLV consists of 100 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by JLV and the functions that collect it are mapped below.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) 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
Report Builder Service Servers 1-4	YES	Yes	SSN/Name/Mailing Address/email/Emergency Contact/Current-Previous Medical record/history	Used for temporary report calling	Stored in an encrypted PDF document for up to 72 hours only
Database Servers 1-3	Yes	Yes	User's Name-ID/PIV/CAC/Patient SSN/Workstation IP Address	Used for audit logging	Stored in an encrypted database controlled by IO
JLV Web Application Servers 1-30	NO	N/A	N/A	N/A	JLV Web Application Servers 1-30
SSOi Servers 1-18	NO	N/A	N/A	N/A	SSOi Servers 1-18

JMeadows Servers 1-25	NO	N/A	N/A	N/A	JMeadows Servers 1-25
VDS Servers 1-20	NO	N/A	N/A	N/A	VDS Servers 1-20

1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

There are two data sources for JLV:
DOD: Composite Health Care System (CHCS) and Bidirectional Health Information Exchange (BHIE)
VA: Veterans Health Information Systems and Technology Architecture (VistA)

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

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.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

JLV disseminates/displays information via electronic transmission from DHA and VA systems. Audit log information and report information are derived from the sources listed above. JLV disseminates/displays information via electronic transmission from DHA and VA systems. Audit log information and report information are derived from the sources listed above.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose. This question is related to privacy control AP-2, Purpose Specification.

JLV 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.

JLV 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.

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

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.

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.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity, and Integrity Board.

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

1.6 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

• Per SORN 24VA10A7 – Patient Medical Records Title 38, United States Code, Section 501(b) and 304.

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

• For the audit log portion of this system, SORN 79VA10 is being updated by VHA privacy to include systems with that functionality. Collection of that data and maintaining the system are authorized by Title 38, United States Code, Section 501.

1.7 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.

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 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 offer assistance to 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 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.

JLV 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 veterans such as: health problems, diagnosis, therapeutic procedures, X-rays, laboratory tests, and operations. -internal/external
Previous Medical Records – Historical medical history and treatment
Patient Race/Ethnicity – statistical reporting
For patient treatment, JLV 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 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

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

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.

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.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

JLV 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.

2.3 How is the information in the system secured?

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

Add answer here:

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.

The SORN for the JLV system is 24VA10A7 and is located at the following website:
https://www.gpo.gov/fdsys/pkg/FR-2012-10-31/pdf/2012-26801.pdf
Amended SORN: https://www.gpo.gov/fdsys/pkg/FR-2014-02-11/pdf/2014-02890.pdf
Amended SORN: https://www.gpo.gov/fdsys/pkg/FR-2014-08-14/pdf/2014-19283.pdf
For the audit log portion of this system, SORN 79VA10 is being updated by VHA privacy to include systems with that functionality. Collection of that data and maintaining the system are authorized by Title 38, United States Code, Section 501.
The security controls for the JLV application cover approximately 17 security areas with regard to 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.

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

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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.

Add answer here:

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.

The SORN for the JLV system is 24VA10A7 and is located at the following website: https://www.gpo.gov/fdsys/pkg/FR-2012-10-31/pdf/2012-26801.pdf

Amended SORN: https://www.gpo.gov/fdsys/pkg/FR-2013-03-22/pdf/2013-06664.pdf
Amended SORN: https://www.gpo.gov/fdsys/pkg/FR-2014-02-11/pdf/2014-02890.pdf
Amended SORN: https://www.gpo.gov/fdsys/pkg/FR-2014-08-14/pdf/2014-19283.pdf

For the audit log portion of this system, SORN 79VA10 is being updated by VHA privacy to include systems with that functionality. Collection of that data and maintaining the system are authorized by Title 38, United States Code, Section 501.

The security controls for the JLV application cover approximately 17 security areas with regard to 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.

JLV user access processes are described below in Section 8. Technical Access and Security
The JLV 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 disseminates/displays the following information 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

JLV 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

JLV 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
- 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.
This question is related to privacy control DM-2, Data Retention and Disposal.

Compensation, pension, and vocational rehabilitation claims folders are retained at the servicing regional office until they are inactive for three years, after which they are transferred to the Records

Management Center (RMC) for the life of the Veteran. Official legal documents (e.g., birth certificates, marriage licenses) are returned to the claimant after copies are made for the claimant's file. At the death of the veteran, these records are sent to the Federal Records Center (FRC) and maintained by the National Archives and Records Administration (NARA) in accordance with NARA policy. Some claims folders are electronically imaged; in which case, the electronic folder is maintained in the same manner as the claims folder. Once a file is electronically imaged and accepted by VBA, its paper contents (with the exception of documents that are the official property of the Department of Defense, and official legal documents), are destroyed in accordance with Records Control Schedule VB–1 Part 1 Section XIII, as authorized by NARA. Documents that are the property of the Department of Defense are either stored at the RMC or transferred to NARA and maintained in accordance with NARA policy. https://www.archives.gov/research.
Vocational Rehabilitation counseling records are maintained until the exhaustion of a Veteran's maximum entitlement or upon the exceeding of a Veteran's delimiting date of eligibility (generally, ten or twelve years from discharge or release from active duty), whichever occurs first, and then destroyed. Automated storage media containing temporary working information are retained until a claim is decided, and then destroyed. All other automated storage media are retained and disposed of in accordance with disposition authorization approved by NARA. Education electronic folders are retained at the servicing Regional Processing Office. Education folders may be destroyed in accordance with the times set forth in the Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII, as authorized by NARA. Employee productivity records are maintained for two years after which they are destroyed by shredding or burning. File information for CAIVRS is provided to HUD by VA on magnetic tape. After information from the tapes has been read into the computer the tapes are returned to VA for updating. HUD does not keep separate copies of the tapes.

JLV 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)? If so, please indicate the name of the records retention schedule.

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.

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 actual defined period will be different depending on the specific record type. VHA Health care facilities do not set record retention periods or disposition authority for PII, nor do they set policy for data destruction. VHA health care facilities are to comply with the VHA RCS 10-1. Additional information can be found at the National Archives Website: https://www.archives.gov/veterans.

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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 Hand Book 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. Have policies and procedures been developed to minimize the use of PII 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 system does not use PII/PHI/SPI or production data for any 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.

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 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 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. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
VISTA	Data is used by JLV 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 Numbers 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
Master Veterans Index (MVI)	Data is used by JLV 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 Numbers 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.
Virtual Lifetime Electronic Record (VLER)	Data service used to bring in data from eHealth Exchange.	Name Social Security Number Date of Birth Mailing Address Zip code Phone Numbers Email Address Emergency Contact Information Current Medications Previous Medical Records	Secure electronic transmission via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS). Storage of report uses AES-256 encryption.

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
		Race/Ethnicity	
VA Veterans Health Administration (VHA)	Patient care	Name Social Security Number Date of Birth Mailing Address Zip code Phone Numbers Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity	Secure application Virtual Private Network (VPN) in Secure Sockets Layer (SSL) /Transport module
VA Veterans Benefit Administration (VBA)	Patient eligibility, benefits	Name Social Security Number Date of Birth Mailing Address Zip code Phone Numbers Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity	Secure application Virtual Private Network (VPN) in Secure Sockets Layer (SSL) /Transport

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.
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 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: This question is #7 in the Privacy Threshold Analysis.

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 data element types such as PII/PHI that are shared/received 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 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 DoD Patient EDIPI DoD User CAC ID/EDIPI	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 24VA10P2 - Patient Medical Records- Title 38 U.S.C.	Secure application VPN in SSL/TLS using FIPS 140-2 certified cryptographic modules
DOD CHCS/AHLTA system	Data is used by JLV to display patient's medical records	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 24VA10P2 - Patient Medical Records- Title 38 U.S.C.	Secure electronic transmission via Transmission Control Protocol (TCP) /Digital Imaging and Communications in Medicine (DICOM). Secure application VPN in SSL/TLS using FIPS 140-2 certified cryptographic module

DOD Bidirectional Health Information Exchange (BHIE)	Data is used by JLV 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	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 24VA10P2 - Patient Medical Records- Title 38 U.S.C.	Secure application VPN in SSL/TLS using FIPS 140-2 certified cryptographic module. Data in temporarily stored user's reports are encrypted using AES-256 bit.
DOD Defense Health Agency (DHA)	Patient care	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 24VA10P2 - Patient Medical Records- Title 38 U.S.C.	Secure application VPN in SSL/TLS using FIPS 140-2 certified cryptographic module
DOD Military Treatment Facility (MTF)	Patient care	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records	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 24VA10P2 - Patient Medical Records- Title 38 U.S.C	Secure application VPN in SSL/TLS using FIPS 140-2 certified cryptographic modules

		Race/Ethnicity		

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

To protect veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:
1. The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.
4. Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

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: 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 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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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. This question is 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.

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways:
1. The System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" 58VA21/22/28 (July 19, 2012). This SORN can be found online at https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02315.pdf
https://www.govinfo.gov/content/pkg/FR-2012-07-19/pdf/2012-17507.pdf
2) This Privacy Impact Assessment (PIA) also serves as notice of the JLV System. 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."
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 through the use of 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 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

VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually-identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. 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

VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually-identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. 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)).

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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 members of the public may not know that the JLV application exists within the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists, as identified in question 6.1, including this Privacy Impact Assessment (PIA) and a System of Record Notice.
Additionally, VHA provides real-time notice at the point of collection as discussed above in section 6.1. VHA permits individuals to agree to the collection of their PII and provides notice on data collection forms and websites.

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?

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.

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).

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.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Individuals (patients) are not given access to their information in JLV. JLV system data is for use by medical service providers only.
As directed in the System of Record Notice (SORN) 24VA10A7 - Patient Medical Records which can be found online at the links noted is section 2.3 above. “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.”

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.

As directed in the System of Record Notice (SORN) 24VA10A7 - Patient Medical Records which can be found online at the links noted is section 2.3 above. “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.”

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.

As directed in the System of Record Notice (SORN) 24VA10A7 - Patient Medical Records which can be found online at the links noted is section 2.3 above. “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.”

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.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Formal redress procedures are provided in SORN 24VA10A7.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

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.

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

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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:
<u>Privacy Risk:</u> There is a risk that individuals may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt.

<u>Mitigation:</u> By publishing this PIA and the applicable SORN, the VA makes the public aware of the unique status of application. The SORN provides the point of contact for members of the public who have questions or concerns about the JLV application.

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?

Describe the process by which an individual receives access to the system.

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

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 is performed through the use of TMS.

For access control, JLV 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. Access to JLV queries and data are restricted further by the following:
VHA users must already have DHA system credentials as well as VistA credentials to use JLV. These systems have their own respective access control process for users to follow.
VBA users must already have VA network access and PIVs but must also request JLV access through CLIN3 processes for access. JLV 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 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 and Rules of behavior 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 for Privacy and HIPAA 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?

If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted,*
2. *Whether it was a full ATO or ATO with Conditions,*
3. *The amount of time the ATO was granted for, and*
4. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

1. Authority to Operate (ATO) granted on 5/13/2021,
2. Yes, ATO with Conditions,
3. 180-day ATO expires on 12/31/2021, and
4. The FIPS 199 classification of the system is MODERATE.

Section 9. 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 provided in this Privacy Impact Assessment is true and accurate.

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2021.08.09 07:40:45 -04'00'

Privacy Officer, Rita Grewal

Andre L. Davis 1130018

Digitally signed by Andre L. Davis 1130018
Date: 2021.08.09 10:54:55 -05'00'

Information Systems Security Officer, Andre Davis

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2021.08.11 13:56:19 -05'00'

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).

https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02315.pdf

https://www.govinfo.gov/content/pkg/FR-2012-07-19/pdf/2012-17507.pdf