PRIVACY IMPACT ASSESSMENT (PIA)

For the

Joint Legacy Viewer (JLV)

Defense Health Agency (DHA)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

□ (1) Yes, from members of the general public.

□ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

□ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

□ **New DoD Information System**	□ **New Electronic Collection**
☒ **Existing DoD Information System**	□ **Existing Electronic Collection**
□ **Significantly Modified DoD Information System**	

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒ **Yes, DITPR**	Enter DITPR System Identification Number	17586 (DMIX)
□ **Yes, SIPRNET**	Enter SIPRNET Identification Number	
□ **No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☒ **Yes** □ **No**

If "Yes," enter UPI UII: 007-000004122 (DMIX)

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** □ **No**

If "Yes," enter Privacy Act SORN Identifier EDHA 07

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

10 U.S.C. Chapter 55, Medical and Dental Care; 42 U.S.C Chapter 117, Subchapters II and III, Reporting of Information, Definitions and Reports; National Defense Authorization Act for Fiscal Year 2014, Pub. L. No. 113-66, Section 525; 32 CFR 199, Civilian Health and Medical Program for the Uniformed Services (CHAMPUS); DoDI 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFs); and E.O. 9397 (SSN), as amended.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The JLV system is a patient-centric, presentation system that pulls information from disparate health-care systems in real time for viewing in a web browser. The web application provides the ability to view specific clinical data within patients' longitudinal health records stored in electronic medical record systems available to the Veterans Administration (VA), Veterans Benefits Administration (VBA) and the Department of Defense (DoD). Authorized users access a patient's clinical data via a web front-end through a browser from within an intranet site.

JLV is a custom Government Off-the-Shelf (GOTS) patient-centric, web presentation system that pulls information from disparate health care systems in real-time for presentation in a browser design.

JLV is available to authorized users throughout DoD, Veterans Benefits Administration (VBA) 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 DoD-issued Common Access Card (CAC) and VA-issued 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 site's 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.

Information is collected from active duty service members and retirees of the seven uniformed services, their family members, survivors, members of the National Guard and Reserves and their families, others who are registered in the Defense Enrollment Eligibility Reporting System (DEERS), and providers. JLV is not the initial point of collection for any personally identifiable information (PII). PII is obtained from existing systems and databases. The personal information retained is as follows:
Patient's name
Patient's social security number
Patient's date of birth
Patient's electronic data interchange personal identifier (EDIPI)
User's name
User's location
User's IP address of the machine where user is logged in
User's organization
User's smart card ID
User's smart card email
Record access date
Event ID and the reason for the access.

The information stored in this system consists of PII protected by the Privacy Act and protected health information (PHI) protected by Health Insurance Portability and Accountability Act (HIPAA). The individuals whose information is stored in this system include active duty military of the seven uniformed services, members of the National Guard and Reserves, veterans, dependents, retirees and/or their dependents, contractors, foreign nationals, former spouses, and prisoners of war.

JLV is accessed at multiple locations by users affiliated with Veterans Administration (VA), Veterans Benefits Administration (VBA), Department of Defense (DoD), Defense Healthcare Management Systems (DHMS) and by users at 105 MTFs. Authorized users access a patient's clinical data via a web front-end through a browser from within an intranet site utilizing NIPRNet to access the system located in the Military Health

System (MHS) Enterprise Services Operations Center (MESOC) San Antonio, Texas. The system does not host a Web site accessible by the public.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The privacy risks associated with the PII/PHI collected are the unauthorized release of PII/PHI data to include identity theft, sharing of PII/PHI with those who have no need to know, unsolicited marketing, and compromise of sensitive information.

To protect patient privacy, only authorized users (e.g., government, military, contractor personnel) with active and valid DoD-issued CAC and VA-issued PIV card can access a patient's clinical data from within an agency's intranet enclave. JLV is not accessible by the public from the Internet. Only individuals with a valid need-to-know demonstrated by assigned official Government duties are granted access. These individuals must satisfy all personnel security criteria with special protection measures or restricted distribution as established by the data owner. Users are expected to adhere to the Privacy Act and HIPAA Privacy Rule when accessing and managing PII/PHI. Systems are maintained in controlled areas accessible only to authorized personnel. Entry into these areas is restricted to those personnel with a valid requirement and authorization to enter. Physical entry is restricted by the use of locks and administrative procedures. The application resides within Military Health System (MHS) Enterprise Services Operations Center (MESOC) and Medical Community of Interest (MEDCOI) perimeter security boundaries. The application only communicates with DoD entities and authorized DoD partners. All communication channels are protected via Secure Sockets Layer (SSL). The application is a viewer and does not permit file upload and all configurations are under Configuration Management control. The operating system has a host based intrusion detection system for further protection.

Data is encrypted in transit to protect against data interception. External threats are mitigated by following Defense Information System Agency (DISA) provided checklists as part of the JLV accreditation efforts under DoD Information Assurance Certification & Accreditation Program (DIACAP) and the DoD Risk Management Framework (RMF). This ensures that all necessary regulations are followed to maintain the security of the JLV system.

Therefore, all applicable security and privacy processes and regulations (e.g., DIACAP, HIPAA, RMF, etc.) required of a DoD system in operation have been defined and implemented, reducing risks to the maximum extent possible and to the point that any remaining risk has been accepted by the JLV Designated Approving Authority (DAA). JLV is currently accredited via a DIACAP with a three year Authority to Operate (ATO).

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify.

Internal DHA organizations, Health Affairs, Personnel & Readiness,
PDWS - Patient Discovery Web Service
DEERS - Defense Enrollment Eligibility Reporting System
VLER - Virtual Lifetime Electronic Record
DES - Data Exchange Services
TMDS - Theater Medical Data Store
CDR - Clinical Data Repository
CHCS - Composite Health Care System
AHLTA
Essentris

☒ **Other DoD Components.**

Specify.

Uniformed Services (Army, Air Force, Navy, Marines), MTFs, Family Support Services, Data Manpower Defense Center

☒ **Other Federal Agencies.**

Specify.

Coast Guard
Public Health Service
Department of Veterans Affairs (VA)
VistA - Veterans Health Information Systems and Technology Architecture
MVI - Master Veteran Index
Veterans Benefits Administration (VBA) to determine veterans' benefits

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Hawaii Resource Group local site support and application support. All employees who have contact with PII/PHI are trained in appropriate handling of PII/PHI in accordance with current DoD regulations and complete annual HIPAA training.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

JLV does not collect PII/PHI directly from individuals; therefore, individuals do not have the opportunity to consent to the collection of their PII/PHI as part of this system. JLV receives PII/PHI from various systems and databases within the DoD and VA which are the collection points for the PII/PHI and provides individuals the opportunity to consent to the collection of their PII/PHI.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

JLV does not collect PII/PHI directly from individuals; therefore, individuals do not have the opportunity to consent to the collection of their PII/PHI as part of this system. JLV receives PII/PHI from various systems and databases within the DoD and VA which are the collection points for the PII/PHI and provides individuals the opportunity to consent to the collection of their PII/PHI.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

□ **Privacy Act Statement** □ **Privacy Advisory**

□ **Other** ☒ **None**

Describe each applicable format.

Although JLV may qualify as a system of records, it is not the initial point of collection for personally identifiable information (PII). JLV collects PII from other systems rather than directly from individuals. Accordingly, a Privacy Act Statement is not required.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.