

PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Longitudinal Natural Language Processing (LNLP)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

11/28/23

Defense Health Management Systems (DHMS)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)

☐ From members of the general public

☐ From Federal employees

☒ from both members of the general public and Federal employees

☐ Not Collected (if checked proceed to Section 4)

b. The PII is in a: (Check one.)

☐ New DoD Information System

☐ New Electronic Collection

☒ Existing DoD Information System

☐ Existing Electronic Collection

☐ Significantly Modified DoD Information System

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

The Department of Defense Natural Language Processing (DoD NLP) application uses a Commercial off the shelf (COTS) Natural Language Processing (NLP) engine (Invenio™) along with Machine Learning (ML) to process free text, creating an "index" of the text in a way that allows for searching concepts with associated context from the original data. The software extracts meaning from free text content (unstructured data) for patient-centered and population health management, enabling better support to Service member and Veteran patient care across both Departments. Success criteria for this includes: 1. Connect to data sources: Pull Community Health Summary Data via the Data Exchange Service (DES) 2. Process data: Process data with NLP in environment and validate search capability 3. Display data: Integrate NLP search capability into hosting system via LNLP Linked Icon The LNLP capability enables granular search of clinical content across data domains. Community Health Summaries (CHS) data, the first source processed with NLP and made available to end-users, often has many documents with inadequately named titles or long documents with large amounts of unstructured free text from community care facilities. Community Health Summary Data and made available for NLP-enabled search during the pilot. Using the LNLP link, clinicians can readily find needed information without manual review. Ultimately, all clinical data domains will be available for NLP-enabled search. Using the LNLP link, clinicians can readily find needed information without slow, manual review. Ultimately, all clinical data domains will be available for NLP-enabled search.

LNLP is accessible by providers from Military Treatment Facilities (MTFs), Medical Centers, Clinics, Hospitals, and VA Treatment Facilities for the provision of healthcare. LNLP is also accessible at multiple locations by users affiliated with the Defense Health Management System (DHMS), such as trainers, engineers, and functional users (clinicians), for development, testing, training, and troubleshooting. The system is not publicly available and can only be accessed by an authorized user with a Common Access Card (CAC) or Personal Identity Verification (PIV) on a DoD or VA network.

LNLP is fed (collects) Electronic Data Interchange Personal Identifiers including home/cell phone, mailing/home address, military records, race/ethnicity, birth date, disability information, DoDID, emergency contact, medical information, name, other ID number, PHI, SSN, sponsor name and insurance information.

LNLP/Joint Legacy Viewer (JLV) does not collect protected health information/personally identifiable information (PHI/PII) directly from individuals and is not the initial point of collection for any PHI/PII, additionally no PII is created or updated. LNLP/JLV is an electronic health record (EHR) viewer that is only capable of receiving PHI/PII from various existing systems and databases within the DoD and VA and displaying them within the JLV/LNLP user interface. PHI/PII is initially 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 collects and stores these data as Portable Document Format (PDF) documents created by a clinician via the JLV ReportBuilder Service. The PDFs are stored in the ReportBuilder secured servers for 72 hours (configurable by the JLV system administrator), after which the PDFs are permanently removed. For auditing

purposes only, JLV retains limited patient PII, such as identifying information and identification numbers, users' log-in related PII, and the reason for each access of the data in accordance with the Health Insurance Portability and Accountability Act (HIPAA). Audit logs are kept for six years.

LNLP is managed by the Federal Electronic Health Record Management office (FEHRM).

d. Why is the PII collected and/or what is the intended use of the PII? (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)

LNLP utilizes patient PHI/PII retrieved from JLV/DES for identification and data matching, enabling clinicians to more quickly and easily review a patient's longitudinal health record, thereby enhancing the timely and comprehensive provision of healthcare services. LNLP does not retain any PHI/PII.

e. Do individuals have the opportunity to object to the collection of their PII? ☐ Yes ☒ No

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

(2) If "No," state the reason why individuals cannot object to the collection of PII.

LNLP/JLV does not collect any PHI/PII directly from individuals and is not the initial point of collection for any PHI/PII, additionally no PII is created or updated. Therefore, individuals do not have the opportunity to object to the collection of their PHI/PII as part of this system.

f. 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.

LNLP processes individuals' PHI/PII collected by JLV and does not directly collect PII/PHI from individuals. Therefore, individuals do not have the opportunity to consent to specific uses of their PHI/PII as part of this system.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.)

☐ Privacy Act Statement ☐ Privacy Advisory ☒ Not Applicable

LNLP processes individuals' PHI/PII collected by JLV/DES and does not directly collect PII/PHI from individuals. Therefore, no Privacy Act Statement or Privacy Advisory is required.

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? (Check all that apply)

☒ Within the DoD Component

Specify. Defense Health Agency (DHA) organizations, Health Affairs, Medical Treatment Facilities, and Personnel & Readiness, Pharmacy Data Warehouse (PDWS)

☐ Other DoD Components (i.e. Army, Navy, Air Force)

Specify.

☐ Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)

Specify.

☐ State and Local Agencies

Specify.

JLV IT

The following language is contained in the contract in accordance with Defense Federal Acquisition Regulation (DFAR) Supplement, Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoDD 5400.11, "DoD Privacy Program," May 8, 2007, and DoD 5400.11-R, "DoD Privacy Program," May 14, 2007.

Personally Identifiable Information (PII) and Protected Health Information (PHI)

The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data. The Contractor shall also ensure the confidentiality, integrity, and availability of Government data in compliance with all applicable laws and regulations, including data breach reporting and response requirements, in accordance with Defense Federal Acquisition Regulation (DFAR) Supplement, Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoDD 5400.11, "DoD Privacy Program," May 8, 2007, and DoD 5400.11-R, "DoD Privacy Program," May 14, 2007. The Contractor shall also comply with federal laws relating to freedom of information and records management.

The TMA Privacy Office website at <http://www.tricare.mil/tmaprivacy/contract.cfm> contains guidance regarding PHI/PII.

The prime contract incorporates FAR 52.224-1 (Privacy Act).

☒ Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)

Specify.

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

Specify.

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

☐ Individuals

☒ Databases

☒ Existing DoD Information Systems

☐ Commercial Systems

☒ Other Federal Information Systems

DoD Information Systems:

Virtual Lifetime Electronic Record (VLER)

Disability Evaluation System (DES)

Theater Medical Data Store (TMDS)

Composite Health Care System (CHCS)

Armed Forces Health Longitudinal Technology Application (AHLTA)

Uniformed Services (Army, Air Force, Navy, Marines),

Family Support Services,

Defense Manpower Data Center (DMDC)

Department of Homeland Security/US Coast Guard (DHS/USCG)

Veteran Affairs/Veteran Benefits/Master Veteran Index/Veterans Health Information Systems and Technology Architecture (VA/VBA/MVI/Vista)

DHA organizations, Health Affairs, Medical Treatment Facilities, and Personnel & Readiness, Pharmacy Data Warehouse (PDWS)

Federal IS:

Pharmacy Data Warehouse (PDWS)

Health and Human Services, US Public Health Service (HHS/PHS)

Database:

Defense Enrollment Eligibility Reporting System (DEERS)

Clinical Data Repository (CDR)

j. How will the information be collected? (Check all that apply and list all Official Form Numbers if applicable)

- | | |
|---|--|
| <input type="checkbox"/> E-mail | <input type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input type="checkbox"/> In-Person Contact | <input type="checkbox"/> Paper |
| <input type="checkbox"/> Fax | <input type="checkbox"/> Telephone Interview |
| <input checked="" type="checkbox"/> Information Sharing - System to System | <input type="checkbox"/> Website/E-Form |
| <input type="checkbox"/> Other (If Other, enter the information in the box below) | |

k. 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 must be consistent.

☐ Yes ☒ No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.d.defense.gov/Privacy/SORNs/>
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

FILE NUMBER: 103-14

DISPOSITION: Temporary. Delete no more than 7 years from the date last modified. (See DoD DTM 22-001 on default disposition policies and OSD Records Manager guidance which file number to associate).

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.

- (1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

10 U.S.C. Chapter 55, "Medical and Dental Care"; 42 U.S.C Chapter 117, Subchapter II, "Reporting of Information" and Subchapter III, "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.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.

(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."

(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

The information collected in this system is for the diagnosis and treatment of medical disorders and does not collect PHI/PII directly from individuals. It is not the initial point of collection for any PHI/PII and is not considered a public information collection IAW DoDM 8910.01, V2, Encl 3, paragraph 8b(5).