

## 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:**

Armed Forces Health Longitudinal Technology Application (AHLTA)

**2. DOD COMPONENT NAME:**

Defense Health Agency

**3. PIA APPROVAL DATE:**

11/15/22

DHA-DAD IO/J-6-SDD-EHR Core Program Management Office (PMO)

### 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 Armed Forces Health Longitudinal Technology Application (AHLTA) is a fully integrated health care information system used in Department of Defense (DoD) Military Treatment Facilities (MTFs) and clinics. It is used to automate and integrate the functions performed by the hospital or other clinical staff and to facilitate the delivery of health care and MTF administration including related Health Insurance Portability and Accountability Act (HIPAA) approved purposes. The military's electronic health record (EHR), AHLTA, is an enterprise-wide medical and archived dental record management system that provides secure online access to Military Health System (MHS) beneficiaries' records. It is used by providers in all fixed and deployed MTFs worldwide. AHLTA integrates Government and commercial off-the-shelf (GOTS/COTS) products by interfacing the existing Automated Information Systems (AIS) with new functionality. Major components of AHLTA include:

Clinical Data Repository (CDR): Centrally stores patient health care history for all service members and beneficiaries. All data (submitted by the beneficiary or modified by the provider) is stored in the AHLTA CDR.

AHLTA Web Print (AWP): Allows the printing of a patient's entire electronic health record with one command and significantly reduces the backlog of records awaiting transfer to the VA system, Social Security Administration, Medical Evaluation Boards and Transition Assistance Programs.

Client Workstation: Allows for comprehensive documentation of patient care.

The enterprise serves over 9.4 million service members, retirees and beneficiaries.

AHLTA collects the following types of personal information about individuals: Demographic information, Protected Health Information (PHI), Contact Information, Spousal Information, Marital Information, and Medical Information.

Personally Identifiable Information (PII), which includes PHI, is collected to determine eligibility, administer health care delivery services, and related HIPAA approved purposes. User data is collected to support administration and clinical practice authorization and access. Clinical patient data is documented and stored in the patient files in AHLTA. This data is used for patient care management. You can search for a patient/retrieve records using PII fields in AHLTA.

The data contained in AHLTA solely concerns MHS beneficiaries for the purpose of providing health care. In emergency situations, DoD facility providers may see members of the general public (non-beneficiaries). The system can accept the existence of a John Doe patient if an individual does not wish to provide PII to receive emergency (life/death or loss of limb/vision) medical care.

AHLTA is owned/operated by Solution Delivery Division/EHR Core PMO.

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)

The PII is collected for authentication, to verify patient eligibility, and to support the delivery of health care to beneficiaries, and to process billing and insurance claims.

The intended use of PII is for authentication, eligibility verification to downstream systems, for data matching the individual with their medical diagnostic reports, to ensure accuracy when these reports are integrated in the medical records for that individual, to support the delivery of health care to TRICARE beneficiaries, and to process billing and insurance claims.

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.

Individuals do not have the opportunity to object to the collection of their PII because AHLTA is not the initial point of collection of the PII.

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.

Individuals do not have the opportunity to consent to the specific uses of their PII because AHLTA is not the initial point of collection of the PII.

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

AHLTA does not collect PII directly 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, Information Operations (J6),  
Solution Delivery Division: EHR Core Program Office,  
Care and Benefits Integrated Systems Program Office  
Electronic Health Record (EHR) Modernization  
Defense Manpower Data Center, DOD Healthcare  
Management System Modernization (DHMSM), Joint  
Operational Medicine Information Systems (JOMIS),  
Enterprise Intelligence and Data Solutions (EIDS)

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

Specify.

Air Force Medical Service, Army Medicine,  
Navy Medicine, Reserve Affairs  
Department of Veteran Affairs  
Department of Homeland Security  
Social Security Administration

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

Specify.

State and Local Agencies

Specify.

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.

Leidos provides Tier 3 support, local site support, and application support. "Leidos shall ensure that its entire staff, including subcontractors and consultants that perform work on this Contract receive training on the Privacy Act, HIPAA, the Alcohol, Drug Abuse and Mental Health Administration (ADAMHA) Reorganization Act, 42 U.S.C. 290dd-2, and the ADAMHA implementing regulations, 42 CFR Part 2.

Leidos shall ensure all employees and subcontractors supply a certificate of all training completion to the Contracting Officer's Representative (COR) within 30 days of being assigned and on an annual basis thereafter.

Leidos shall not use or further disclose PII other than as permitted or required by the Contract or as Required by Law.

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

Specify. Health Information Exchanges - CommonWell and eHealth Exchange

**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

System interfaces with Defense Enrollment Eligibility Reporting System (DEERS), Composite Health Care System (CHCS), Clinical Data Repository/ Health Data Repository (CHDR), Theater Medical Data Store (TMDS), and Pharmacy Data Transaction Service (TPharm), Navy Medicine on Line (NMO), Air Force Complete Immunization Tracking Application (AFCITA), Medical Protection System (MEDPROS), Corporate Dental Application (CDA).

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

E-mail

Official Form (Enter Form Number(s) in the box below)

In-Person Contact

Paper

Fax

Telephone Interview

Information Sharing - System to System

Website/E-Form

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    EDHA 07

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.    N1-330-11-001, item 1

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

(3) Retention Instructions.

911-17 (AHLTA/CHCS) Temporary. Cut off upon last episode of patient care or last entry to the patient record is annotated. Destroy 75 years after cutoff.

**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.

Public Law 104-191, Health Insurance Portability and Accountability Act of 1996; 10 U.S.C., Ch. 55, Medical and Dental Care; 10 U.S.C. 1097a, TRICARE Prime: Automatic Enrollments; 42 U.S.C. 290dd, Substance Abuse Among Government and Other Employees; 42 U.S.C. 290dd-2, Confidentiality Of Records; 42 U.S.C. Ch. 117, Sections 11131-11152, Reporting of Information; 45 CFR 164, Security and Privacy; Department of Defense (DoD) Instruction 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFS); DoD Manual 6025.18, Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs; 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.

An OMB Control Number is not required because the system is not the entry point for all the information collected and the other data is collected through non-standardized methods.