



PRIVACY IMPACT ASSESSMENT (PIA)

For the

AHLTA

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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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
- 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

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

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; 32 CFR 199.17, TRICARE Program; DoDI 6015.23, Delivery of Healthcare at Military Treatment Facilities: Foreign Service Care; Third-Party Collection; Beneficiary Counseling and Assistance Coordinators (BCACs); 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.

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 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.

Local Cache Server (LCS): Contains an Oracle database which allows encounter data to be stored and accessed when the CDR is not available. The LCS also syncs data, authenticates users and provides HyperText Transfer Protocol Secure (HTTP(S))-based communications between the LCS and other subsystems.

Client Work Station: Allows for comprehensive documentation of patient care.

CommVault (a COTS product): Cyber Security policy requires encryption of mobile devices and removable media that is Federal Information Processing Standards (FIPS) 140-2 compliant. CommVault was identified to meet enterprise needs for encryption of backup data and recovery. In 2013, CommVault was implemented to replace Acronis as the AHLTA Local Cache Servers (LCS) FIPS 140-2 compliant back-up solution. Current implementation includes modules to backup online MTF data and archive data remotely.

AHLTA collects the following types of personal information about individuals:

Name

Social Security Number (SSN)

Truncated SSN

Defense Enrollment Eligibility Reporting System (DEERS) Patient ID

Gender

Citizenship

Race/Ethnicity

Birth Date

Home Telephone Number

Personal Cell Phone Number

Military Record

Mailing/Home Address

Religious Preference

Spouse Information

Marital Status

Medical Information

Emergency Contact

Personal E-mail Address

Personally identifiable information (PII), which includes protected health information (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.

The data contained in AHLTA is solely collected from and 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.

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

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

There are privacy risks inherent in any system that collects, uses, and shares PII/PHI (e.g., risks associated with unauthorized, malicious, accidental disclosure, and modification or destruction of information; unintentional errors and omissions; IT disruptions due to natural or man-made disasters; and failure to exercise due care and diligence in the implementation and operation of the IT system). However, all applicable security and privacy processes and regulations (e.g., DoD 8570.01_M, DoD Risk Management Framework (RMF), Health Insurance Portability and Accountability Act (HIPAA), etc.) have been defined and implemented to reduce privacy related risks to the maximum extent possible.

Access to the Trusted Computing Base (TCB) for AHLTA at the MTF and Defense Information Systems Agency (DISA) is restricted to System Administrator(s) who are responsible for setting up user accounts and assigning user permissions. The system architecture security requirement ensures that the system security safeguards are protected from access, modification, and destruction by unauthorized personnel. The security safeguards that enforce the previously described security requirements are considered the TCB and are enforced by the AHLTA application. AHLTA also uses Common Access Cards (CAC) and Public Key Infrastructure (PKI) as part of its access control measures.

Access to the Operating System (OS) for software maintenance and support is restricted to the MTF, DISA, and Tier 3 support staff.

The DISA and MTF computer facilities housing the AHLTA application and network communication servers have comprehensive physical, personnel, and administrative controls in accordance with local policies. Additionally, safeguards are in place within MTFs to prevent unauthorized physical access to local AHLTA workstations. Office door locks, password-enabled screen savers, staff monitoring, application time-outs, and AHLTA technical controls prevent unauthorized individuals from accessing information on unattended workstations.

Two levels of AHLTA annual training are in place for MTFs, DISA, and DoD Vendors:

1. Awareness-level: Awareness training is provided to all users and staff of the AHLTA system. The objective of awareness training is to build a working knowledge of principles, concepts, and practices of Cyber Security. Awareness training ensures that all users, including managers and senior executives, are exposed to basic information system security policies, guidance and breaches (e.g., HIPAA security policy, Privacy Act of 1974).

2. Performance-level: Specific guidance will be provided to personnel who design, implement, use, and maintain the AHLTA system and resources. Security training provides system managers, system administrators, and other personnel with access to system-level software, the knowledge and skills to implement appropriate safeguards as a component of their assigned duties.

As reasonable and appropriate, employees will receive training that includes:

- Protection from malicious software: guarding against, detecting, and reporting malicious software;
- Log-in monitoring: monitoring log-in attempts and reporting discrepancies; and
- Password management: creating, changing, and safeguarding passwords.

At the performance level, the training incorporates information concerning users' roles and responsibilities. For example, in selecting a password of appropriate strength, changing the password periodically (if required), and

safeguarding one's password. The training will include information for staff members so that they are cognizant of the importance of timely application of system patches to protect against malicious software and exploitation of vulnerabilities.

AHLTA displays a DoD approved warning banner and system use notification message before granting system access to potential users. A warning banner is displayed to all users who have access to AHLTA resources. The banner warns both authenticated and authorized users that their activities may be monitored and recorded in case data needs to be collected for an investigation. Users must acknowledge the military health system Cyber Security (MHS CS)-mandated Security Banner before they are allowed to authenticate to the system.

The following specific Privacy Act warning is included in the DoD approved warning banner:

"Information contained in this system is subject to the Privacy Act of 1974 (5 U.S.C., 522 as amended). Personal information contained in this system may be used only by authorized persons in the conduct of official business. Any individual responsible for unauthorized disclosure or misuse of personal information may be subject to a fine of up to \$5,000."

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.

MHS: Composite Health Care System (CHCS), Clinical Data Repository/Health Data Repository (CHDR), Theater Medical Data Store (TMDS), Virtual Lifetime Electronic Record (VLER), Healthcare Artifact and Image Management Solution (HAIMS), Pharmacy Data Transaction Service (TPHarm), and closely related systems.

Other DoD Components.

Specify.

Defense Manpower Data Center: Defense Enrollment Eligibility Reporting System (DEERS) is the source system for patient demographics, enrollment, and eligibility data.

Defense and Veterans Eye Injury and Vision Registry (DVEIVR) provides a registry for the Department of Defense Vision Center of Excellence (VCE) to improve clinical care for our Service Members and Veterans.

Service level systems: Navy Medicine on Line (NMO), Air Force Complete Immunization Tracking Application (AFCITA), Medical Protection System (MEDPROS), Corporate Dental Application (CDA), Medical Operational Data, and other closely related systems.

United States Coast Guard (USCG) has access based upon the local site agreements that allow USCG providers access to AHLTA to view data and order labs at DoD facilities.

Other Federal Agencies.

Specify.

To the Department of Veteran Affairs for the purpose of enabling DoD data retrieval from the Federal/Bi-Directional Health Information Exchange (FHIE/ BHIE) frame-work, sharing of clinical data to facilitate care at joint facilities like the James A. Lovell Federal Health Care Center (JALFHCC) and other closely related systems.

Social Security Administration assists with the assignment of benefits.

State and Local Agencies.

Specify.

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

Specify.

Leidos provides Tier 3 support, 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.

Health Information Exchanges and Other Health Insurance Providers

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.

In accordance with the Privacy Act of 1974, submission of information is voluntary. If an individual chooses not to provide their information, no penalty may be imposed, but absence of the requested information may result in administrative delays.

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

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.

Consent to the specific uses of PII is obtained as necessary, in accordance with DoD 5400.11-R, DoD Privacy Program, C4.1.3. PHI is collected for permitted uses and disclosures as set forth by DoD 6025.18-R, DoD Health Information Privacy Regulation. Individuals are informed of these uses and are given the opportunity to restrict the use of their PHI based on the procedures in place at the local facility where the data is collected and maintained, in accordance with DoD 6025.18-R, C10.1.

For uses other than Treatment, Payment and Healthcare Operations, individuals can authorize the use of their PHI by submitting DD Form 2870. For uses other than Treatment, Payment and Healthcare Operations, individuals can request restrictions on the use of the PHI by submitting DD Form 2871.

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

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

- | | |
|--|--|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

AUTHORITY: 10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR 199.17, TRICARE Program; DoDI 6015.23, Delivery of Healthcare at Military Treatment Facilities: Foreign Service Care; Third-Party Collection; Beneficiary Counseling and Assistance Coordinators (BCACs); and E.O. 9397 (SSN), as amended.

PURPOSE: To collect information from you in order to determine your eligibility for health care, deliver and manage that care, and manage the entities providing that care.

ROUTINE USES: Information in your records may be disclosed to private physicians and Federal agencies, including the Departments of Veterans Affairs, Health and Human Services, and Homeland Security in connection with your medical care; other federal, state, and local government agencies to determine your eligibility for benefits and entitlements and for compliance with laws governing public health matters; and government and nongovernment third parties to recover the cost of healthcare provided to you by the Military Health System.

Any protected health information (PHI) in your records may be used and disclosed generally as permitted by the HIPAA Privacy Rule (45 CFR Parts 160 and 164), as implemented within DoD. Permitted uses and disclosures of PHI include, but are not limited to, treatment, payment, and healthcare operations.

APPLICABLE SORN: The SORN Applicable to this system is EDHA07, Military Health Information System.

DISCLOSURE: Voluntary. If you choose not to provide your information, no penalty may be imposed, but absence of the requested information may result in administrative delays.

The following PAS may be provided in lieu of the above PAS when orally collecting information from an individual. If the individual requests additional information about the authorities, purposes, routine uses, or disclosures, that section of the above PAS should be read. If the individual requests a paper copy of the PAS, the individual may choose whether to withhold any responses until a paper copy of the above PAS has been provided.

I am about to request information from you in order to determine your eligibility for health care, deliver and manage that care, and manage the entities providing that care. If you choose not to provide this information, no penalty may be imposed, but absence of the requested information may result in

administrative delays.

Collection of this information is permitted by authorities including 10 U.S.C. Chapter 55. It may be disclosed in connection with your medical care; to determine your eligibility for benefits and entitlements; for compliance with laws governing public health matters; and to recover the cost of healthcare provided to you. It may also be disclosed for reasons compatible with why it was collected and when permitted by the HIPAA Privacy Rule and other applicable privacy laws. Would you like to know more about the authorities, purposes, routine uses, or disclosures, or receive a paper copy of the full Privacy Act Statement?

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.