



PRIVACY IMPACT ASSESSMENT (PIA)

For the

AHLTA

TRICARE Management Activity (TMA)

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
- 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

MHS Beneficiaries

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 C.F.R. 199.17 TRICARE Program; 45 C.F.R. Parts 160 and 164, Health Insurance Portability and Accountability Act Privacy and Security Rules; DoD 6025.18-R, DoD Health Information Privacy Regulation; DoDI 6015.23, Delivery of Healthcare at Military Treatment Facilities; DoDD 6040.37, Confidentiality of Medical Quality Assurance; and, E.O. 9397 (as amended, SSN).

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 staff and to facilitate the delivery of health care and MTF administration.

AHLTA collects the following types of personal information about individuals:

Name

Social Security Number (SSN)

Defense Enrollment Eligibility Reporting System (DEERS) Patient ID

Gender

Citizenship

Race/Ethnicity

Birth Date

Home Telephone Number

Religious Preference

Spouse Information

Marital Status

Medical Information

Emergency Contact

Personally identifiable information (PII), which includes protected health information (PHI), is collected to determine eligibility and administer health care delivery services. 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 about MHS beneficiaries for the purpose of providing health care. In emergency situations, DoD facilities may see members of the general public. The system can accept the existence of a John Doe patient if an individual does not wish to provide PII.

While AHLTA does not host a web site accessible by the public, in the future, a sub-portion of the AHLTA system (i.e., eForms) will become accessible to TRICARE beneficiaries via the TRICARE Online (TOL) portal.

The system point of contact is:

AHLTA Product Manager

5113 Leesburg Pike, Suite 701

Falls Church, VA 22041

(703) 681-7143

(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 collecting, using, and sharing PII/PHI (e.g., unauthorized malicious or accidental disclosure, modification, or destruction of information; unintentional errors and omissions; IT disruptions due to natural or man-made disasters; 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 Information Assurance Certification & Accreditation (DIACAP), Health Insurance Portability and Accountability Act (HIPAA), etc) have been defined and implemented, reducing this risk to the maximum extent possible.

Access to the Trusted Computing Base (TCB) for AHLTA at the Military Treatment Facility (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.

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. Safeguards preventing unauthorized physical access to AHLTA workstations within the MTFs are included. Office door locks, password-enabled screen savers, monitoring by facility staff, application time-outs, and AHLTA technical controls that prevent unauthorized individuals from logging onto the system provide protection for unattended workstations.

There are two levels of annual training that occur at the MTFs, DISA, and DoD Vendors for AHLTA described below:

1. Awareness-level: Awareness training is provided to all users and staff of the AHLTA system. A result of this awareness training is to build a working knowledge of principles, concepts, and practices that are implemented in Information Assurance. Awareness training ensures that all users, including managers and senior executives, are exposed to basic information system security awareness materials such as the consequences of non-compliance with the HIPAA security policy. Security awareness training also encompasses instruction on the 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 ensures that system managers, system administrators, and other personnel with access to system-level software have adequate technical training to perform their assigned duties.

As reasonable and appropriate, employees and users will be trained regarding procedures for the following:

- 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 authorized and unauthorized 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 information assurance (MHS IA)-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.

Composite Health Care System (CHCS), Clinical Data Repository/Health Data Repository (CHDR), Theater Medical Data Store (TMDS) and Pharmacy Data Transaction Service (PDTs), Clinical Data Mart (CDM), Navy Medicine on Line (NMO), Air Force Complete Immunization Tracking Application (AFCITA), Medical Protection System (MEDPROS), Corporate Dental Application (CDA),

Dental Common Access System (DENCAS), Optical Fabrication Automated Management System (OFAMS)

Other DoD Components.

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

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.

State and Local Agencies.

Specify.

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

Specify.

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.

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 in 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 C.F.R. 199.17 TRICARE Program; and, E.O. 9397 (as amended, SSN).

PURPOSE: To provide automated and integrated functionality to the hospital staff and to facilitate the delivery of health care and Military Treatment Facilities administration. Collected personally identifiable information is solely from MHS beneficiaries, and is used to determine eligibility, administer health care delivery services and for patient care management.

ROUTINE USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a (b) of the Privacy Act of 1974, the DoD "Blanket Routine Uses" under 5 U.S.C. 552a (b) (3) apply to this collection. The applicable System of Record Notice further describes disclosures outside DoD, such as disclosures to the Department of Veterans Affairs for the purpose of providing medical care to former Service members, and disclosures to local and state governments and agencies for compliance with laws governing communicable disease control, child abuse and other public health matters. Disclosures do not include individually identifiable health information unless permitted by the HIPAA Privacy Rule and other applicable law.

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.