



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Theater Medical Data Store (TMDS)

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
- 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. 131, Office of the Secretary of Defense; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; Chapter 55 sections 1074 and 1104 ; 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.

TMDS is a web-based application that serves as the authoritative theater database for collecting, distributing and viewing Service members' pertinent medical information. It provides one central location for healthcare providers to view theater medical data supporting the Defense Health Information Management System (DHIMS) mission to seamlessly capture, manage, and share healthcare data for electronic health records (EHR). The medical information within TMDS comes primarily from Theater Medical Information Program-Joint (TMIP-J) feeder systems such as AHLTA-Theater and TMIP Composite Health Care System Cache (TC2). TMDS also has a graphical user interface which does allow patient demographics to be directly entered. TMDS provides viewing and tracking of ill or injured patients as they are evacuated through the levels of care while in theater. TMDS contains standard patient demographics on all military members, active, guard and reserve, foreign nationals, and contractors who receive healthcare at military treatment facilities.

The system collects the following personally identifiable information (PII) and protected health information (PHI) about individuals:

Name
Age
Birth date
Social Security Number (SSN)
Marital status
Personal cellphone number
Home telephone number
Address
Race
Pay grade
Personnel code
Service ID number
Mobilization status
Unit ID
Unit phone number
Medical information

TMDS has a front end Graphical User Interface but it is only accessible to approved users and not the general public. Approved users may access the site with their web browser but only from .mil domain.

The system is owned by:
Force Health Protection and Readiness (FHP&R)
5113 Leesburg Pike, Suite 900
Falls Church, VA 22041
(800) 497-6261

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

The risk is limited to authorized users who knowingly divulge personally identifiable information (PII)/protected health information (PHI). This type of risk is virtually impossible to prevent, considering individual trust is placed in each employee who is granted access. If a breach of trust occurs the individual's access would be terminated immediately, and they would be disciplined and likely be removed from employment with DHIMS.

The loss of PII/PHI is mitigated through network firewall and account management for need-to-know tiered-access. TMDS users are required to have Health Information Portability and Accountability Act (HIPAA) training in order to be granted the privilege and role of viewing PII/PHI. Patient demographic information is available for viewing but only for those who require access to perform their duties. Employees are required to sign a non-disclosure

agreement in order to work at DHIMS. In addition, highly sensitive medical information is limited to a smaller group of healthcare providers.

The system is classified as a networked, mission critical, Sensitive But Unclassified (SBU) system, and a DoD Mission Assurance Category (MAC) II.

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.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

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.

As a reminder, although Patient Administrators can enter data into TMDS, the majority of information comes from TMIP-J Systems such as AHLTA-Theater and TMIP Composite Health Care System Cache (TC2). Submission of PII is voluntary. If an individual chooses not to provide information, no penalty may be imposed, but absence of the requested information may result in delays in providing treatment or other administrative delays. PII collected is for the purpose of ensuring that accurate care is provided to the right individual.

(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.

On the occasion that TMDS is the data entry point, individuals will be given the opportunity to consent to the specific uses of their PII. In accordance with DoD 5400.11-R and DoD 6025.18-R, individuals are given the opportunity to consent to or authorize the specific uses of their PII/PHI at the point of collection.

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.

- Privacy Act Statement**
- Privacy Advisory**
- Other**
- None**

Describe each applicable format.	<p>Individuals are advised concerning the use of their PII. All advisories are verbal.</p> <p>PRIVACY ACT STATEMENT</p> <p>AUTHORITY: 10 U.S.C. 1074, Medical and Dental Care for Members and Certain Former Members; 10 U.S.C. 1104, Sharing of Health-Care Resources with the Department of Veterans Affairs; 45 CFR Parts 160 and 164, Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules; and E.O. 9397 (SSN), as amended.</p> <p>PURPOSE: The information collected is used to provide one central location for healthcare providers to seamlessly view, capture, manage, and share theater medical data on all military members, active, guard and reserve, foreign nationals, and contractors who receive healthcare at military treatment facilities.</p> <p>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. Information may be shared with Department of Veterans Affairs, federal, state, local, or foreign government agencies, and with private business entities, including individual providers of care and third party payers on matters relating to eligibility and claims pricing, including payment for health care services provided to foreign nationals and contractors at military treatment facilities, fraud, program abuse, utilization review, quality assurance, peer review, program integrity, third-party liability, coordination of benefits, and civil or criminal litigation.</p> <p>DISCLOSURE: Voluntary. If you choose not to provide your information, no penalty may be imposed, but absence of the requested information may result in delays in providing treatment or other administrative delays.</p>
----------------------------------	---

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.