PRIVACY IMPACT ASSESSMENT (PIA)

For the

Theater Medical Data Store (TMDS)
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**
- ☐ **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: 1228 (TMIP-J)
- ☐ **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 UII: 007-000001913 (TMIP-J)

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 EDHA 05

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	Pending approval from IMCO for paperwork reduction compliance
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; DoDI 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFs); 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.

Theater Medical Data Store (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 health care providers to view theater medical data supporting the Defense Healthcare Management Systems (DHMS) mission to seamlessly capture, manage, and share health care 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 (AHLTA-T) and Composite Health Care System Cache (TC2). TMDS also has a graphical user interface (GUI) which allows the user to enter patient demographics directly into the system. TMDS provides viewing and tracking of patients as they move through the continuum of care while in theater. It contains standard patient demographics on all military members (active, guard, and reserve), foreign nationals, detainees, and contractors who receive or have received medical or dental care at one or more DoD military treatment facilities (MTFs) in theater. Lastly, TMDS serves as a host for the Theater Blood program. Theater Blood provides visibility and a traceable record of transient patients' blood transfusions, blood inventory, and blood donations according to the theater facility and location.

The system collects the following personally identifiable information (PII) and protected health information (PHI) about individuals:
Name
Other names used
DoD Identification Number (DoD ID)
Other ID Number
Citizenship
Age
Gender
Date of Birth
Social Security Number (SSN)
Marital status
Spouse Information
Personal cellphone number
Home telephone number
Emergency Contact
Mailing Address
Race/Ethnicity
Religious preference
Disability Information
Military records (Pay grade, Personnel code, Service Identification number, Mobilization status, Unit Identification, Unit phone number)
Medical information

TMDS has a front end GUI, 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 a .mil domain.

The system is owned and managed by Health Readiness Policy & Oversight (formerly Force Health Protection & Readiness).

(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 PII/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, they would be disciplined and likely be removed from employment with DHA.

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 those who require access to perform their duties and have the approved permission to view it. Employees are required to sign a non-disclosure agreement in order to work at DHMS. In addition, highly sensitive medical information is limited to a smaller group of healthcare providers.

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. Military Health System

☒ **Other DoD Components.**

Specify. Defense Manpower Data Center's Defense Enrollment and Eligibility Reporting System (DEERS)
Defense Finance and Accounting Services (DFAS)
Defense and Veterans Eye Injury and Vision Registry (DVEIVR)

☒ **Other Federal Agencies.**

Specify. The Veteran's Administration through Bi-Directional Health Information Exchange (BHIE) Framework, Data Exchange Service (DES) and others as directed.
Combat Injury Pay (CIP)

☐ **State and Local Agencies.**

Specify.

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

Specify. Various contractors develop, operate and maintain the system for the Government. The following contractors have access to the information:

Akimeka
Booz Allen Hamilton
Deloitte
Data Network Corporation - DNC
SeKON

All must maintain the appropriate background investigations based on their specific roles and responsibilities.

The contract requires the developer, DNC, to "establish appropriate administrative, technical, and physical safeguards to protect any and all Government data, to ensure the confidentiality, integrity, and availability of government data. At a minimum, this shall include provisions for personnel security, electronic security and physical security."

☐ **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.

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

TMDS does not collect PII/PHI directly from individuals; therefore, individuals do not have the opportunity to object to the collection of their PII/PHI as part of this system. PII/PHI is received from TMIP-J applications via system to system interface, which are the initial collection points for the PII/PHI and provides individuals the opportunity to object to the collection of their PII/PHI.

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.

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

TMDS does not collect PII/PHI directly from individuals; therefore, individuals do not have the opportunity to consent to the collection of their PII/PHI as part of this system. PII/PHI is received from TMIP-J applications via system to system interface, which are the initial collection points for the PII/PHI and provides individuals the opportunity to consent to the collection of their PII/PHI.

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.	TMDS is a system of records under the Privacy Act of 1974. However, because TMDS does not serve as the initial point of collection for any records it contains, no Privacy Act Statement is required.

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.