PRIVACY IMPACT ASSESSMENT (PIA)

For the

Military Health System (MHS) Data Repository (MDR)
TRICARE Management Activity

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: 140
- ☐ **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 007-000000510

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 DHA 07

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.

5 U.S.C. 301, Departmental regulations; 10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); 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.

MDR is the centralized data repository for MHS health care data and is the cornerstone of Defense Health Services Systems (DHSS). The MDR implements a semi-automatic, event driven data collection system that has the ability to quantify, qualify and report on all data received by the MDR. This data is received from various feed nodes from more than 260 Department of Defense (DoD) health data network systems worldwide on a weekly and monthly processing schedule. MDR normalizes the data by processing each data type against MHS business rules; stores the data (e.g., DHSS maintains more than 5 billion records on-line with 10+ years of data); and provides the data to users via DHSS data marts and/or transmits the data to approved external recipient offices/systems/organizations/agencies to enable crosscutting analysis among financial, clinical, enrollment and eligibility, purchased care databases and for clinical research studies to identify and follow best practice.

Data are collected on beneficiaries of the DoD Health System including Direct care and Purchased Care systems. Specific private data elements collected are:
Name
Social Security Number (SSN)
Other ID Number - EDIPN (Electronic Data Interchange Person Number)
Gender
Race/Ethnicity
Birth Date
Mailing/Home Address
Home Telephone Number
Religious Preference
Spouse Information
Marital Status
Child Information
Medical Information
Disability Information
Emergency Contact
Employment Information

The MDR is in the Operations and Maintenance phase, where the necessary post-implementation and in-process reviews of a production environment are conducted to safeguard privacy. The system is considered sensitive but unclassified. MDR access is available to the various TMA agencies; Branches of Service (Army, Navy, Air Force, and Coast Guard); Department of Veterans Affairs (DVA) and Veterans Health Administration (VHA); and the following contractors: Corporate Users (Business & Economic Analysis Division (BEA) under the Office of the Chief Financial Officer (OCFO) & contractors, Concurrent Technologies, and TRICARE Encounter Data (T) Next Generation (TNEX) contractors. The language across all contracts is that provided by the respective U.S. Army Medical Research Acquisition Activity, Fort Detrick, Maryland, Contracting Officers in the form of approved BAA (Business Associate Agreement) after they have been vetted through the various administrative, technical, and physical security controls in place to safeguard beneficiary personally identifiable information (PII) and protected health information (PHI). The system is not web-based therefore, does not host a Web site accessible by the public.

MDR is owned by the Defense Health Services Systems Program Executive Office (DHSS PEO). Contact information is as follows:

Program Name: MDR
POC Title: Branch Chief, Business Intelligence
Program Address: 7700 Arlington Blvd, Suite 5101 Falls Church, VA 22042
Program Telephone Number: (703) 681-1141
Program Email: DHSS2@tma.osd.mil

A full PIA has been previously submitted and signed on May 20, 2010.
The system is not covered by a Data Sharing Agreement (DSA) or Data Use Agreement (DUA).

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

The privacy risks associated with personally identifiable information (PII) and protected health information (PHI) collected is the risk of disclosure when users fail to lock their workstations when not in use or a hacker breaking into the system and stealing the PII/PHI. These risks are mitigated through the implementation of various administrative, technical and physical security controls, such as the use of Common Access Card (CAC) with required 2-factor authentication including a pin created by the user, use of Secure Sockets Layer to access the MDR environment, implementation of Role-based access control within the application, and security awareness training requirement. Risks regarding the collection, use and sharing of PII/PHI in the system have been minimized through system design and implementation of various administrative, technical, and physical security controls.

Also, system users are required to submit an Account Authorization Request Form (AARF) and have the need for access validated. Only users with demonstrated need to know receive access to MDR.

In the area of I&A the AIX (Advanced Interactive eXecutive) OS (operating system) maintains and authenticates all MDR user ID's and passwords. All password operations (e.g.; creation, change) submitted to the OS, or checked by the OS (e.g.; expiration, suspension, deletion), are processed by routines native to the OS. The MDR Audit template includes all events regarding user I&A actions (e.g.; logon, logoff, switch user (su) operations, successful/ unsuccessful, etc.).

DHSS requires that all individuals requesting access to MDR data take annual HIPPA and Security/Information Awareness Training and file the Certification of Completion with the DHSS PEO Access Office. The MDR server and its components are housed at DISA Oklahoma City. Physical access to the MDR server and its components are controlled by DISA. Users, data recipients, operators and system administrators connect to the server through secured virtual private networks (VPNs) and/or secure network protocols (e.g. SSH/SFTP) utilizing FIPS 140-2 compliant encryption.

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. PII/PHI will be shared within TMA and Service Groups (Army, Navy, Air Force, and Coast Guard)

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. DVA, VHA (Department of Veterans Affairs, Veterans Health Administration)

☐ **State and Local Agencies.**

Specify.

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

Specify. Corporate Users (Defense Health Cost Assessment and Program Evaluation (DHCAPE) Division under the Office of the Chief Financial Officer (OCFO) & contractors, Concurrent Technologies, and TRICARE Encounter Data (T) Next Generation (TNEX) contractors. The language across all contracts is that provided by

the respective U.S. Army Medical Research Acquisition Activity, Ft. Detrick, Maryland, Contracting Officers in the form of approved BAA (Business Associate Agreement). All Business Associate Agreements shall comply with The Health Insurance Portability and Accountability Act, which requires physicians to have their business associates; claims processors or third-party billers agree to protect personally identifiable information.

☐ **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.

Information is not collected directly from the individual. However, a process is in place for individuals to access, question, and correct their information in the system through the Privacy Act System of Records Notice (SORN) published in the Federal Register. The SORN provides individuals with the information on how to review/access 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.

A process is in place for individuals to access, question, and correct their information in the system through

the Privacy Act System of Records Notice (SORN) published in the Federal Register. The SORN provides individuals with the information on how to review/access their PII.

Protected health information (PHI) is only used and disclosed as permitted by DoD 6025.18-R, DoD Health Information Privacy Regulation. As permitted by DoD 6025.18-R, the PHI is used for business purposes, therefore, an authorization is not required for this use of 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.

In accordance with DoD 5400.11-R, individuals are informed of what information about them is stored on the system through publication of a Privacy Act System of Records Notice in the Federal Register.

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.