PRIVACY IMPACT ASSESSMENT (PIA)

For the

Military Health System (MHS) Management Analysis and Reporting Tool (MART) (M2)

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 140 (EI / DS)

□ **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: 007-000000117 (EI / DS)

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 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.

10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR 199, Civilian Health and Medical Program for the Uniformed Services (CHAMPUS); 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.

The Military Health System (MHS) Management Analysis and Reporting Tool (M2) contains data extracted from the MHS Data Repository (MDR). The application is built to support analysts in the conduct of studies for MHS leadership in the management and oversight of MHS operations. M2 combines a powerful commercial ad hoc query and reporting tool Business Objects (BO) with MHS data originating from clinical, financial, and beneficiary demographic domains. M2 data are accessed to perform trend analyses, conduct patient and provider profiling studies, and realize opportunities for transferring health care from the private sector to the MTF. M2 includes inpatient, outpatient, and ancillary direct and purchased care data as well as eligibility and enrollment data. These integrated data enhance data-driven analysis by decision-makers at all levels of the MHS. M2 is accessible via a user-friendly, client-server interface.

The purpose of the M2 data mart includes:

1) facilitating practice of proactive health care management (e.g., preventive medicine, managed care) for beneficiaries enrolled at Military Treatment Facilities (MTFs);

2) building and editing reports to facilitate decision-making and support strategic planning;

3) identifying patients for disease management programs and monitoring patients' use of services;

4) conducting patient and provider profiling studies;

5) analyzing utilization management data (e.g., Emergency Room (ER) visits per 1,000 enrollees, preventable admission rates); and

6) conducting "make vs. buy" analyses.

Personally Identifiable Information (PII) / Personal Health Information (PHI) that will be maintained, stored, or transmitted includes personal descriptors, identification numbers, ethnicity, health, employment, and life information.

PII / PHI is collected the following categories of individuals and can be retrieved using any element or set of elements mentioned above:

- Active duty, reserve, veterans, and retiree military (all services, including the Coast Guard and National Guard)
- Dependents (including present, former, and surviving children and spouses)

A PIA has been previously submitted for this system with a final signature date of May 9, 2012.

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

There are three privacy risks within M2.

1) If a person was to be able to spoof the identity of a user – specifically the CAC credentials of an Administrator – then the person could gain access to the PII / PHI.

2) If a user was to download PII/PHI to their laptop into a spreadsheet, then they could transport the PII/PHI off-site and the PII/PHI would be at risk for theft.

3) Printing M2 data and not properly disposing of it.

All users are made aware of these risks via the Information Assurance (IA) awareness training they have to pass in order to receive an account on M2. M2 users with access to PII / PHI are required to submit the DHSS Account Access Request Form (AARF) and complete the approval process before obtaining access to patient level data. Users are required to complete an annual EI / DS User Security Awareness Training Class, store data only on encrypted devices, and comply with all HIPAA data use safeguards.

Additionally, M2 receives and uses the minimum PII / PHI necessary to conduct the functions to which the system has been authorized. Risks regarding the use of PII / PHI in the system have been minimized through system design and implementation of various administrative, technical, and physical security controls.

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. TRICARE Regional Offices (TRO), TRICARE Overseas Area Offices (TAO), DHA Directorates

☒ **Other DoD Components.**

Specify. Tri-Services

☒ **Other Federal Agencies.**

Specify. Veteran Administration (VA) through the Federal Health Information Exchange (FHIE) feed

☐ **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.

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

M2 is not the initial point of collection of PII / PHI from individuals; therefore, individuals do not have the opportunity to object to the collection of their PII / PHI.

M2 receives data from MDR, which collects PII / PHI directly from individuals and provides individuals the opportunity to object at the point of collection.

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.

M2 is not the initial point of collection of PII / PHI from individuals; therefore, individuals do not have the opportunity to consent to the collection of their PII / PHI.

M2 receives data from MDR, which collects PII / PHI directly from individuals and provides individuals the opportunity to consent at the point of collection.

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.

M2 is not the initial point of collection of PII / PHI from individuals; therefore, no privacy act statement or privacy advisory 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.