PRIVACY IMPACT ASSESSMENT (PIA)

For the

Protected Health Information Management Tool (PHIMT)
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: 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: 007-000000510 (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 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 (Department Regulation); 10 U.S.C. 55 (Medical and Dental Care); 45 C.F.R. 160 and 164, Parts A and E (Health Insurance Portability and Accountability Act of 1996); DoD 6025.18-R (DoD Health Information Privacy Regulation); 10 U.S.C. 1071-1085 (Medical and Dental Care); 42 U.S.C. 117, Sections 11131-11152 (Reporting of Information); DoD Instruction 6015.23 (Delivery of Healthcare at Military Treatment Facilities (MTFs)); DoD 6010.8-R (CHAMPUS); 10 U.S.C. 1095 (Collection from Third Party Payers Act); and E.O. 9397 (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.

PHIMT provides the Military Health System (MHS) with a web-based application, (HIPAA Privacy Accelerator (HPA)), that simplifies and automates many of the provisions of HIPAA Privacy. PHIMT is used to track disclosures of patient health information and provide reports of those disclosures, upon request, to the patient. PHIMT can also be used to document patient privacy complaints, disclosure accounting suspensions and restrictions, health information disclosure authorizations, and restrictions to Protected Health Information (PHI).

The types of personally identifiable information (PII) and PHI collected in the system include:
Name
Social Security Number (SSN)
Truncated SSN
Other ID Number - Electronic Data Interchange Person Numbers (EDIPN)
Race/Ethnicity
Religious Preference
Gender
Marital Status
Spouse Information
Mailing/Home address
Birth Date
Home Telephone Number
Medical Information

PHIMT is in its Operational/maintenance life cycle phase. It is an administrative system and has been designated a MAC III system under DoD Instruction 8500.2, Information Assurance (IA) Implementation. TMA owns a licence for the application and it is operated by Military Health System (MHS). The application hosts a Web site that is Public Key enforced and accessible only by authorized users using Common Access Card (CAC).

Application point of contact:
PHIMT Project Controller
5203 Leesburg Pike, Sky 2 Suite 900
Falls Church, VA 22041

(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 PII/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), use of Secure Sockets Layer to access PHIMT 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 are also minimized through system design and implementation of various administrative, technical, and physical security controls.

Additionally, account creation is approved through an Account Authorization Request Form (AARF) submission via the Electronic CAC Registration Service(ECRS) and acceptance where by a single sign on is accepted by PHIMT using the account holders EDIPN.

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, and Air Force, and Coast Guard) for the purpose of recording disclosures, suspensions, restrictions, reports and letters, authorizations, notices, complaints and accounting of disclosures.

☐ **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.

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

PHIMT 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. PHIMT receives PII/PHI from the Military Health System Data Repository (MDR) or from validated PHIMT users.

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.

PHIMT 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. PHIMT receives PII/PHI from the MDR or from a authorized PHIMT user interface.

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.

A Privacy Act Statement (PAS) is not necessary in connection with most of the information collected into this system. However, since DoD may request that individuals authorize the disclosure of their own medical or dental information, a PAS should be provided in connection with that authorization. Individuals who want to authorize the disclosure of their medical or dental records should complete DD Form 2870, Authorization for Disclosure of Medical or Dental Information, Dec 2003.

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.