PRIVACY IMPACT ASSESSMENT (PIA)

For the

Theater Medical Information Program - Joint: Maritime Medical Modules (MMM)
Department of the Navy - DHA DHP Funded System - BUMED

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 164(UnderTMIP-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

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 N06150-2

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.

SORN authorities:

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 1095, Collection from Third Party Payers Act
10 U.S.C. 5131 (as amended)
10 U.S.C. 5132; 44 U.S.C. 3101
10 CFR part 20, Standards for Protection Against Radiation
E.O. 9397 (SSN), as amended.

Other authorities:

42 CFR 290DD Drug and Alcohol Treatment Records
5 CFR 293.502, Subpart E, Employee Medical File System Records
29 CFR Part 5, Labor Standards
5 CFR 339.101-306, Coverage
DoDD 6485.1 Human Immunodeficiency Virus-1 (HIV-1)
DoD 6025.18-R, Health Information Privacy Regulation

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 purpose of Maritime Medical Modules (MMM) is to continue the ongoing need for commandant, area commanders, and field level commanding officers to assess medical operational readiness within legacy environments. This relationship is based on the ability of MMM to:

- Store, process, and retrieve HIPAA data
- Monitor the operating site's medical environment
- Support medical supply management

The types of personally identifiable information (PII) about individuals collected in the system include: Name, truncated SSN, SSN, personal cell and home telephone numbers, mailing/home address, emergency contact, birth date, Citizenship, Gender, Race/Ethnicity, Birth Date, Place of Birth, Biometrics: Height/Weight, Religious Preference, Military Records (User Type (Active or Reserve), User ID, Rank, Pay Grade, Command Info (address, UIC)), Spouse Information, Child Information, and Medical Information. More details on subcategories of information collected are provided in section 3. a.(1).

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

All systems are vulnerable to "insider threats". Maritime Medical Modules (MMM) managers are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. There are defined criteria to identify who should have access to MMM. These individuals have gone through extensive background and employment investigations.

The MMM program is always evaluating risks in safeguarding data in the application. MMM does, at a minimum, an annual review of its DoDI 8500.01, and DoDI 8510.01 application security controls and follows Office of Management and Budget (OMB) Communications- 202-395-7254, and Best Practices. In an effort to make the federal government's identity theft awareness, prevention, detection, and prosecution efforts more effective and efficient, the OMB, along with the Department of Homeland Security (DHS), employs a list of best practices to help agencies improve the security and privacy of their information systems. This is incorporated into the MMM Information Assurance (IA) testing. Each risk listed in the Certification report to the Navy Authorization Official (NAO), in categories ranging from security and privacy training for personnel to procurement issues, is associated with selected best practices and important resources to help MMM mitigate and avoid these risks. These artifacts, submitted in the DoD Information Assurance Certification and Accreditation Process (DIACAP) package are evaluated to provide the best possible safeguards of privacy information.

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. Existing DoD information systems: Navy Medicine On-Line (NMO), HIV Management System Loader (HMSL), Theater Medical Information Program Framework (TMIP- Framework) - Master Cluster Management Service (TMIP - Framework - MCMS), Armed Forces Health Longitudinal Technology Application - Theater (AHLTA-T), Naval Dosimetry Center (NDC)

☐ **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.

Contractor: CACI

Excerpts from the contract:

* Comply with all HIPAA and Privacy Act requirements.

* Follow all DUA and DoD requirements for secure disposal, destruction, and/or sanitization of all equipment that contained PHI.

* The contractor shall ensure that data which contains PHI is continuously protected from unauthorized access, use, modification, or disclosure. The contractor shall comply with all previously stated requirements for HIPAA, Privacy Act, Federal Information Security Management ACT (FISMA), Personnel Security, Electronic Security, and Physical Security, and ensure that the concepts in the DoD Global Information Grid (GIG) are interwoven throughout its efforts.

☐ **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.

In the case of military personnel, the requested information is mandatory because of the need to collect immunization and other preventive health data. Reference DoD I 6025.19, IMR provides guidance for collecting identifiable patient data that directly affects Medical Readiness. SECNAVINST 6230.4 requires all immunization and other preventive health data of military members be entered into DEERS and be maintained in a repository within the Department of the Navy. As such, the service member is required to provide the appropriate PII. This immunization data is used to determine the Medical Readiness of the individual service member and the operational unit to which the service member is attached. NAVMED P-5055 Radiation Health program requires collection of radiation health exposure data.

In the case of all other personnel/beneficiaries, the requested information is voluntary. If the requested information is not furnished, comprehensive health care may not be possible, but care will not be denied.

(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.

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

In the case of military personnel, there is no opportunity for individuals to object/consent to collection of immunization and other preventive health data.

Members· are verbally counseled regarding the collection of data as mandated in 0001 6025.19, Individual Medical Readiness (IMR), and SECNAVINST 6230.4. NAVMED P-5055 Radiation Health program requires collection of radiation health exposure data.

In the case of other personnel/beneficiaries, the information is used for medical treatment purposes.

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 is maintained in the physical medical record of each individual.

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.