PRIVACY IMPACT ASSESSMENT (PIA)

For the

Electronic Deployment Health Assessment
Department of the Navy - TMA 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
- ☐ **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, Health Care Services Incurred on Behalf of Covered Beneficiaries: Collection from Third Party Payers Act
10 U.S.C. 5131 (as amended), Bureau: Name, Location;
10 U.S.C. 5132, Bureau: Distribution of Business, orders, records, expense;
44 U.S.C. 3101, Record Management by Agency Head;
10 CFR part 20, Standards for Protection Against Radiation
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)
6025.18R, DoD Health Information Privacy Regulation.
E.O. 9397 (SSN), as amended

Other authorities:

10 U.S. C. 55 Medical and Dental Care

42 CFR 290DD Drug and Alcohol Treatment Records

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.

EDHA is a web-based tool accessed by users through a secure https website, created using Microsoft .net. The data are stored at NMCPHC in a MS SQL environment. The system is used by service members in order to complete Deployment Health Assessments as mandated by BUMED and the DoD. The surveys are used in order to determine and create a record of any deployment limiting conditions that the deployer may be experiencing, as well as deployment related health issues. The surveys are completed by the service member, after which, a provider must review and certify the form. Provider access is restricted to medical departments of the Coast Guard, Army, Navy, Air Force, and Marine Corps, those in the public health reporting chain according to BUMED and OPNAV instructions and Immediate Supervisors in Command (ISICs). All with system access, other than service members logging in to complete assessments, must submit a SAAR-N form and be screen by the eDHA Help Desk prior to being granted access to the system.

Types of personal information that is collected by the system includes: Name, Personal Cell Telephone Number, Mailing/Home Address, Marital Status, Birth Date, Home Telephone Number, Medical Information: general health assessment with a YES/NO response (medical board status, pregnancy, supply of medication, prescription glasses, mental health counseling); physical health problems, emotional problems, general health, wounded (yes/no response), list of symptoms (trouble breathing, fever, diarrhea, skin diseases, etc. (yes/no); Social Security Number, Gender, Emergency Contact, and Personal Email Address.

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

Where as all systems are at risk and vulnerable to unauthorized access or intrusions such as hacking the eDHA data are processed on an accredited network in the Navy Medicine domain in accordance to DoD requirements and authorized by Designated Approving Authority at NETWARCOM. The risk that eDHA data could be compromised has been evaluated and determined to acceptable because the system has been properly secured with the appropriate administrative, technical and physical safeguards listed in this PIA.

The eDHA user risk concern is considered acceptable because all users are required to initially complete and annually re-take DoD approved training for Privacy Act, HIPAA, and security awareness that addresses privacy issues, system use and information management.

All DoD users must be "Suitable" for employment before gaining any DoD system access. System access is controlled by an approved SAAR-N form (DD form 2875). A SAAR-N form can only be submitted for a user by their "Chain of command" authority. A user login ID is only issued after the SAAR-N is endorsed, validated and approved but the command Security Manager. Additionally, eDHA user access is restricted to those personnel who also meet the "Need to Know" access requirement and who carry out a public health function including Medical Departments, those in the public health reporting chain according to BUMED, OPNAV instructions, and ISICs

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. Personnel supporting Navy and Marine Corps public health surveillance responsibilities

☒ **Other DoD Components.**

Specify. Coast Guard Army, Air Force, and Army

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify. LHI Logistic Health Incorporated , OSD/HA contract. Disclosure is only to to authorized agencies with which a data use agreement has been properly executed.

All contractors has a Business Associates Agreement as part of their contract to prevent disclosure of PII.

☐ **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.

The DoD forms used to design eDHA require service member to submit at least demographic data as a way to track compliance. The member can opt out of any other information.

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.

Use of an individual's PII for public health purposes are set forth in the Privacy Act of 1974 and DoD Health Information Privacy Regulation (DoD 6025.18-R) issued pursuant to the Health Insurance Portability and Accountability Act of 1996. DoD 6025.18-R may also place additional procedural requirements on the uses and disclosures of such information.

No use of the information not authorized by current regulation is intended, therefore no requirement for individual consent pertains. NMCPHC is a public health entity and is authorized to use collected PII for public health acitivities.

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.

The Privacy Act Statement appears at the beginning of the deployment health assessment form before PII is collected.

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.