PRIVACY IMPACT ASSESSMENT (PIA)

For the

NAVY MARINE CORPS PUBLIC HEALTH CENTER - EPIDATA CENTER PUBLIC HEALTH SUREVEILLANCE SYSTEM (NMCPHC-EDC2)
Department of the Navy - BUMED - DHP Funded System

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: DITPR ID: 17795
- ☐ **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: 007-000100726

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 N06150-2 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.

This system is used by officials, employees and contractors of the Department of the Navy (and members of the National Red Cross in naval Military Treatment Facilities) in the performance of their official duties relating to the health and medical treatment of Navy and Marine Corps members; physical and psychological qualifications and suitability of candidates for various programs; personnel assignment; law enforcement; dental readiness; claims and appeals before the Council of Personnel Boards and the Board for Correction of Naval Records; member's physical fitness for continued naval service; litigation involving medical care; performance of research studies and compilation of statistical data; implementation of preventive medicine programs and occupational health surveillance programs; implementation of communicable disease control programs; and management of the Bureau of Medicine and Surgery's Radiation program and to report data concerning individual's exposure to radiation.

This system is also used for the initiation and processing, including litigation, of affirmative claims against potential third party payers.

Personally identifiable information (PII) collected about individuals include: Name, SSN, DoD ID Number, Gender, Race/Ethnicity, Birth Date, Place of Birth, Home Telephone Number, Personal Email Address, Mailing/Home Address, Unit Identification Code (UIC), and rank.

(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 system data is processed on an accredited network in the Navy Medicine domain in accordance to DoD requirements and authorized by Designated Approving Authority at Naval Network Warfare Command (NETWARCOM). The risks that the system's data could be compromised have been evaluated and determined to acceptable because the system has been properly secured with the appropriate administrative, technical, and physical safeguards listed in the PIA.

The system's user risk concern is considered acceptable because no users have access to the data unless an employee of the NMCPHC EpiData Center Information Technology (IT) staff with a National Agency Check with Law and Credit (NACLC), biometric, Common Access Card (CAC), and access to the NMCPHC accredited network has been granted. In addition personnel complete Cybersecurity Awareness, Privacy Act, and Health Insurance Portability and Accountability Act (HIPAA) training on an annual basis that addresses privacy issues, system uses and information management.

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. Navy and Marine Corps personnel supporting NMCPHC

☐ **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. Booz Allen and Hamilton and Battelle Memorial Institute. All contracts have Business Associate Agreements (BAA) clause that restrict access and use of PII.

☒ **Other** (e.g., commercial providers, colleges).

Specify. Internships From Eastern Virginia Medical School

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 System does not directly collect PII from individuals.

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.

The System does not directly collect PII from individuals.

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 System does not directly collect PII from individuals.

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.