PRIVACY IMPACT ASSESSMENT (PIA)

For the

Navy Disease Reporting System internet (NDRSi)
Department of the Navy - BUMED - TMA 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	
☐	**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.

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; and, E.O. 9397 (SSN), as amended.

International Health Regulations (2005), Executive Order (United States) 13295 of April 4, 2003, Executive Order (United States) 13375 of April 1, 2005 mandates the need to do medical surveillance (including disease reporting) to prevent the introduction, transmission, or spread of communicable disease.

DODD 6490.02E "Comprehensive Health Surveillance", Joint Publication 4-02 "Doctrine for Health Service Support for Joint Operations", and CJCS Memorandum MCM 0028-07 "Procedures for Deployment Health Surveillance" require service components to conduct medical surveillance in support of Force Health Surveillance and specifies the timely collection of reportable medical events as an important component of that surveillance.

Navy Manual of the Medical Department p-117 articles 2-17 and 2-19 and BUMED INST 6220.12B and Triservice Reportable Events Guidelines and Case Definitions specifically set forth requirements of medical reporting in the Navy, mandating the collection and maintenance of Medical Event Reports in NDRSi.

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.

By DOD directive, the services are required to collect medical event reports (MERs) for over 70 specific medical diagnoses and events and forward these reports to the Armed Forces Health Surveillance Center for DOD-wide collation. These events are reportable due to: their mission degrading potential, our ability to prevent the illness by establishing specific control measures, or their potential for rapid spread causing significant outbreaks. In the Department of Navy and Coast Guard, NDRSi captures and archives medical event reporting data per the directives and regulations mentioned above.

NDRSi is a web-based tool accessed by users through a secured https website, created via .net. The data is stored at Navy and Marine Corps Public Health Center (NMCPHC), Portsmouth, VA in a SQL environment. User access is restricted to Medical Departments, those in the public health reporting chain according to BUMED and OPNAV instructions and Immediate Supervisors in Command (ISICs).

As account holders, local Navy and Marine Corps units providing inpatient or outpatient care log into NDRSi and fill out a MER for a reportable event. In the MER, the following information is collected: information specific to an individual (identifiable information including social security number and name), epidemiologic information pertaining to risk (including date of birth, gender, beneficiary category) and public health control measures (such as travel history, vaccine history, chemoprophylaxis).

(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 NDRSi data is processed on an accredited network in the Navy Medicine domain in accordance to DoD requirements and authorized by Designated Approving Authority at NETWARCOM. The system is secured with the administrative, technical and physical safeguards listed in this PIA.

Users with a defined "need to know" 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 by the command Security Manager. Additionally, NDRSi 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. United States Air Force School of Aerospace Medicine, Army Public Health Command, Armed Forces Health Surveillance Center

☐ **Other Federal Agencies.**

Specify.

☒ **State and Local Agencies.**

Specify. State and local public health agencies

☐ **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.

NDRSi does not collect PII directly from the patient - it is is not the source system.

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.

NDRSi does not collect PII directly from the patient - it is is not the source system.

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.	NDRSi does not collect PII directly from the patient - it is is not the source system

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.