



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Human Immunodeficiency Virus Management System (HMS)

Department of Navy - 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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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

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.

System of Record 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; and, E.O. 9397 (SSN)

Additional Authorities:

Department of Defense Instruction (DoDI) Number 6025.19, "Individual Medical Readiness," January 3, 2006

DODI 6485.01, "Human Immunodeficiency Virus (HIV)," October 17, 2006

SECNAV Instruction 5300.30D, "Management of HIV Infection in the Navy and Marine Corps," January 3, 2006

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.

HMS is a web-based information management system and data repository service. It is used to conduct infectious disease-related administrative reporting; patient tracking, and to maintain an Infectious Disease on-line transaction processing (OLTP) and data warehouse service to access, validate, and conduct statistical analysis. It provides the storage, reporting, and management of Department of Defense (DoD) HIV test results. It allows the Navy Central Human Immunodeficiency Virus (HIV) Service (NCHP) to maintain a secure database system for query, review, and validation of all HIV test results; clinical HIV treatment history; rapid generation of notification letters and generation of detail and summary reports within specified time frames. The system allows NCHP personnel, authorized Bureau of Naval Personnel (BUPERS) staff and HIV Evaluation and Treatment Units (HETU) clinical staff secure HMS access to perform all necessary functions that provide life-cycle historical tracking of test results, notification, and clinical treatment processes. The system is designed to enable supported DoD organizations to share common information and provide a historical repository of test results and related demographics data from government-contracted laboratories, Defense Manpower Data Center (DMDC), DoD personnel systems, Composite Health Care System (CHCS), the Medical Readiness Reserve System (MRRS), and the Armed Forces Health Surveillance Center (AFHSC).

HMS accepts infectious disease test orders from CHCS, Shipboard Automated Medical System (SAMS) and MRRS. It receives test results from laboratory contractors for upload back into CHCS. It also receives additional infectious disease (RetroViral) related test orders from the CHCS. NCHP uses this information to screen Armed Forces personnel for readiness, conduct studies and statistical analysis.

Personal information collected on individuals include: personal information, including name, gender, birth date, social security number, medical information and military records.

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

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that HMS, with its extensive collection of PII, could be compromised. Because of this possibility, appropriate administrative, physical and technical controls listed in this PIA are in place.

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.

Commanding Officers, SAMS Sites, and authorized registered HIV Evaluation and Treatment Unit personnel and between DoD information systems - Medical Readiness Reporting System (MRRS), HCS, BUPERS

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.

This is a requirement of DoD/DoN. IAW DoD 5400.11-R, a requirement to furnish personal data is mandatory when the DoD Component is authorized to impose a penalty on the individual for failure to provide the requested information. Upon entrance into military service with the Department of Defense, individuals are asked to provide their SSNs. The SSN becomes the service or employment number for the individual and is used to establish personnel, financial, medical, and other official records.

Reference DoD 6025.19 Individual Medical Readiness (IMR) for collecting data.

For this purpose Armed forces personnels cannot deny the collection of this data; however, beneficiaries are required to sign a consent form prior to collection. Electronic data collection systems will capture, track and report each member's IMR currency. Military Department-specific systems must interact with key enterprise IM/IT systems, such as the Defense Enrollment Eligibility Reporting System and the MHS Central Data Repository/Warehouse, to facilitate data exchange between Military Departments. Additionally, such systems must interface with other line readiness-related reporting systems, such as the MRRS.

Currently each of these systems require PII to accurately identify Armed Forces Personnel.

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.

Non-Consensual conditions of disclosures within the DoD. Records pertaining to an individual may be disclosed to a DoD official or employee provided:

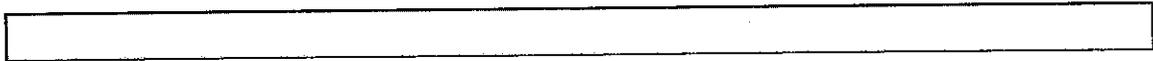
- The requester has a need for the record in the performance of his or her assigned duties. The requester shall articulate in sufficient detail why the records are required so that the custodian of the records may make an informed decision regarding their release;
- The intended use of the record generally relates to the purpose for which the record is maintained; and
- Only those records as are minimally required to accomplish the intended use are disclosed. The entire record is not released if only a part of the record will be responsive to the request.
- Rank, position, or title alone does not authorize access to personal information about others.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

A pre-printed Department of Defense (DD) Form 2005, "Privacy Act Statement - Health Care Records" is provided to the patient at the point of care for review and signature and it is placed in the patient's medical record.



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.