

PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Theater Medical Information Program - Joint Increment 2 Release 3 (I2 R3)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

07/26/24

JOMIS

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)

- ☐ From members of the general public ☐ From Federal employees
- ☒ from both members of the general public and Federal employees ☐ Not Collected (if checked proceed to Section 4)

b. The PII is in a: (Check one.)

- ☐ New DoD Information System ☐ New Electronic Collection
- ☒ Existing DoD Information System ☐ Existing Electronic Collection
- ☐ Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The I2 R3 electronically bridges documentation of healthcare delivery in the "Theater of Conflict" to the sustaining base, captures clinical information and other data and passes it to the Theater Medical Data Store (TMDS), where it can be viewed by users all over the world. Data is sent to repositories for enterprise use by Military Health System (MHS) stakeholders. I2 R3 contains protected health information (PHI) and personally identifiable information (PII), consist of custom of the shelf (COTS) and government of the shelf (GOTS) and custom coded software components.

The system collects the following PII and PHI about individuals. PII/PHI is collected to determine eligibility and administer health care delivery services. User data, which contains some PII and PHI, is collected to support administration and clinical practice authorization and access. Clinical patient data is documented and stored in the patient files. Data is used for patient care management.

Personally identifiable information (PII) and protected health information (PHI) collected includes: personal descriptors, ethnicity, contact information, identification numbers, life, education, employment, financial, social security number, and health information.

Categories of individuals about whom the Personally Identifiable Information (PII) and Protected Health Information (PHI) is collected for the system/electronic collection include active duty military (all services + Coast Guard and Reserve), veterans, dependents, retirees and/or their dependents, contractors, foreign nationals, former spouses, reservist, National Guard personnel, and prisoners of war.

The TMIP-J I2 R3 system is located at Military Treatment Facilities close to combat zones where the system is used to support force health protection, casualty care and detainee care. The TMIP-J I2 R3 application is used on Hospital Ships to support force health protection, casualty care and provide humanitarian assistance. TMIP-J I2 R3 is accessed at these locations by users affiliated with the Department of Defense Health Agency. TMIP-J I2 R3 is installed, and managed by the component military service personnel responsible for the facility and supported, and owned by the Joint Operational Medical System (JOMIS) Program Management Office (PMO).

d. Why is the PII collected and/or what is the intended use of the PII? (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)

PII/PHI is collected to determine eligibility and administer health care delivery services. Data is used for patient care management; administer health care delivery services, support the functions of patient contact, correct identification of patients, patient tracking, etc. User data is collected to support administration and clinical practice authorization and access.

e. Do individuals have the opportunity to object to the collection of their PII? ☒ Yes ☐ No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Submission of information is voluntary, individuals may object or request restrictions on the use of PII/PHI by submitting DD 2871.

f. 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.

Individuals are informed of these uses and are given the opportunity to consent or restrict the use of their PHI. For uses other than treatment, payment and healthcare operations, individuals authorize the use of their PHI by submitting DD 2870.

PII collection is mandatory for US military personnel. However, for other patients choosing to not provide PII, care will not be denied.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.)

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

AUTHORITY: 10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); DoDI 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFs); and E.O. 9397 (SSN), as amended.

PURPOSE: To collect information from you in order to determine your eligibility, as well as document and administer delivery of health care within the theater environment.

ROUTINE USES: Information in your records may be disclosed to private physicians and Federal agencies, including the Departments of Veterans Affairs, Health and Human Services, and Homeland Security in connection with your medical care; other federal, state, and local government agencies to determine your eligibility for benefits and entitlements and for compliance with laws governing public health matters; and government and non-government third parties to recover the cost of healthcare provided to you by the Military Health System. For a full listing of the Routine Uses, please refer to the applicable SORN.

Any protected health information (PHI) in your records may be used and disclosed generally as permitted by the HIPAA Privacy Rule (45 CFR Parts 160 and 164), as implemented within DoD. Permitted uses and disclosures of PHI include, but are not limited to, treatment, payment, healthcare operations, and the containment of certain communicable diseases.

For a full listing of the applicable Routine Uses, refer to the applicable SORN: EDHA 07, Military Health Information System (78 FR 69076) located at: <http://dpcl.d.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570672/edha-07/>

DISCLOSURE: Voluntary. If you choose not to provide your information, no penalty may be imposed, but absence of the requested information may result in administrative delays.

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? (Check all that apply)

☒ Within the DoD Component

Specify. Defense Health Agency: TMDS

☒ Other DoD Components (i.e. Army, Navy, Air Force)

Specify. Defense Finance and Accounting Services (DFAS); Defense and Veterans Eye Injury and Vision Registry (DVEIVR); Defense Manpower Data Center (DMDC) is the source system for patient demographics, enrollment, and eligibility data.

☒ Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)

Specify. The Veteran's Administration through Bi-Directional Health Information Exchange (BHIE) Framework; Data Exchange Service (DES) and others as directed; Combat Injury Pay (CIP); Department of Veteran Affairs for the purpose of enabling DoD data retrieval from the Federal / Bi-Directional Health Information Exchange (FHIE/ BHIE) frame-work; Departments of Health and Human Services (HHS); Department of Homeland Security (DHS)

☐ State and Local Agencies

Specify.

☒ Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)

Specify.

Various contractors develop, operate and maintain the system for the Government. The following contractors have access to the information: American Systems Corporation (ASC); Planned Systems International; 2C4 Technologies

All must maintain the appropriate background investigations based on their specific roles and responsibilities. The contract requires the developer, ASC, to "establish appropriate administrative, technical, and physical safeguards to protect Government data, and ensure the confidentiality, integrity, and availability of government data. At a minimum, this shall include provisions for personnel security, electronic security and physical security." Cybersecurity requirements: Information Systems: The employee shall comply with DoDI 8582.01 "Security of Unclassified DoD Information on Non-DoD Information Systems" and "Cybersecurity" and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53/53a and NIST SP 800-37, Risk Management Framework (RMF) Guide for Applying the Risk Management Framework to Federal Information Systems, as well as emerging DoD Cybersecurity policy designed to address evolving threats.

☐ Other (e.g., commercial providers, colleges).

Specify.

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

☒ Individuals

☐ Databases

☒ Existing DoD Information Systems

☐ Commercial Systems

☐ Other Federal Information Systems

Theater Medical Data Store (TMDS)

j. How will the information be collected? (Check all that apply and list all Official Form Numbers if applicable)

☐ E-mail

☐ Official Form (Enter Form Number(s) in the box below)

☒ In-Person Contact

☐ Paper

☐ Fax

☐ Telephone Interview

☒ Information Sharing - System to System

☐ Website/E-Form

☐ Other (If Other, enter the information in the box below)

k. 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 must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier

EDHA07

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.dod.mil/Privacy/SORNs/>
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

I. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.

GRS 5.2, item 020 (DAA-GRS-2022-0009-0002)

(2) If pending, provide the date the SF-115 was submitted to NARA.

N/A

(3) Retention Instructions.

FILE NUMBER: 103-14

DISPOSITION: Temporary. Delete no more than 7 years from the date last modified. (See DoD DTM 22-001 on default disposition policies and OSD Records Manager guidance which file number to associate).

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.

(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

10 USC Chapter 55, Medical and Dental Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); DoDI 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFs); and EO 9397 (SSN), as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.

(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections."

(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

The information collected in this system is for the diagnosis and treatment of medical conditions and is not considered a public information collection per DoDM 8910.01, V2, Encl 3, paragraph 8b(5).