

# 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:**

Joint Operational Medicine Information Systems Operational Medicine Care Delivery Platform (JOMIS OPMed CDP)

**2. DOD COMPONENT NAME:**

Defense Health Agency

**3. PIA APPROVAL DATE:**

4/24/2024

Joint Operational Medicine Information Systems (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.**

Joint Operational Medicine Information Systems Operational Medicine Care Delivery Platform (JOMIS OPMed CDP) is a hybrid system hosted in Cloud One and deployed to local workstations for use in disconnected, intermittent, and low-communication (DIL) environments providing mission-critical data services and management key to the (JOMIS) program management office (PMO) efforts to modernize operational medicine (OPMed). JOMIS OPMed CDP enables healthcare delivery at the disease of non-battle injury (DNBI) documentation, damage control resuscitation (DCR) at Roles 1 and 2 (Role 1: First response medical care, Role 2: provides advanced trauma management and emergency medical treatment including continuation of resuscitation started in Role 1), and damage control surgery (DCS) at Role 2. The JOMIS OPMed CDP provides both passive and active clinical decision support, management of patient data transmitted to OMDS (Operational Medicine Data Service), is DIL compliant and communicates with the Battlefield Assisted Trauma Distributed Observation Kit (BATDOK) solution.

The deployed application enables a tiered user experience across roles of care using a comprehensive and easy-to-use platform that specializes in configurable and scalable healthcare workflow and content delivery; asynchronous and synchronous collaboration; and user-driven, multi-modal, and modern user interfaces.

Personally identifiable information (PII) and protected health information (PHI) is collected to provide health care services. The types of PII collected in this system include: contact information, military information, demographic information, and Protected Health Information (PHI). 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.

Categories of individuals about whom the PII and PHI is collected and stored in this system include: active-duty military (all services + Reserve), Coast Guard, National Guard, contractors, foreign nationals, and prisoners of war.

**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)

The PII is collected for identification, verification, and data matching. The intended use of the PII is to enhance healthcare services for injuries sustained in deployed combat zones.

**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. If an individual chooses not to provide PII/PHI information, no penalty may be imposed, however, absence of the requested information may result in treatment delays.

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.

Consent to the specific uses of PII is obtained as necessary, per DoD 5400.11-R, DoD Privacy Program, C4.1.3. PHI is collected for permitted uses and disclosures as set forth in DoD Manual (DoDM) 6025.18, Implementation of the HIPAA Privacy Rule in DoD Health Care Programs. Individuals are informed of these uses and are provided the opportunity to restrict the use of their PHI based on procedures in place at the local facility where the data is collected and maintained, per DoDM 6025.18.

For uses other than treatment, payment and healthcare operations, individuals may authorize the use of their PHI by submitting DD2870 or request restrictions on the use of the PHI by submitting DD Form 2871.

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

Patients are requested to sign a Privacy Act Statement (DD Form 2005) which is maintained in the patient record.

This statement serves to inform you of the purpose for collecting personal information required by JOMIS OPMed and how it will be used.

AUTHORITY: 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 E.O. 9397 (SSN), as amended.

PURPOSE: To collect information to determine your eligibility, document and provide 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 system of records notice (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 <http://dpcl.d.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570672/edha-07/>

DISCLOSURE: Mandatory for US Military members; voluntary for all others. If you choose not to provide your information, no penalty may be imposed, however, absence of the requested information may result in administrative or treatment 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)

- |  |          |  |
|--|----------|--|
| <input checked="" type="checkbox"/> Within the DoD Component   | Specify. | <input type="text" value="DHA Military Treatment Facilities"/>     |
| <input checked="" type="checkbox"/> Other DoD Components (i.e. Army, Navy, Air Force)  | Specify. | <input type="text" value="Army, Navy, Air Force and Marine Corp"/> |
| <input checked="" type="checkbox"/> Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)   | Specify. | <input type="text" value="US Coast Guard"/>                        |
| <input type="checkbox"/> State and Local Agencies  | Specify. | <input type="text"/>   |
| <input type="checkbox"/> 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. | <input type="text"/>   |
| <input type="checkbox"/> Other (e.g., commercial providers, colleges).   | Specify. | <input type="text"/>   |

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

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> Individuals                      | <input type="checkbox"/> Databases          |
| <input checked="" type="checkbox"/> Existing DoD Information Systems | <input type="checkbox"/> Commercial Systems |

Other Federal Information Systems

DEERS, OMDS and MHS Genesis

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

- |   |  |
|---|--|
| <input type="checkbox"/> E-mail   | <input type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input checked="" type="checkbox"/> In-Person Contact                             | <input type="checkbox"/> Paper   |
| <input type="checkbox"/> Fax  | <input type="checkbox"/> Telephone Interview                                   |
| <input type="checkbox"/> Information Sharing - System to System                   | <input type="checkbox"/> Website/E-Form  |
| <input type="checkbox"/> Other (If Other, enter the information in the box below) |  |

N/A

**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

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

**l. 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.

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

(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.

Public Law 104-191, Health Insurance Portability and Accountability Act of 1996; 10 USC Ch. 55, Medical and Dental Care; 10 USC 1097a, TRICARE Prime: Automatic Enrollments; Payment Options; 10 USC 1097b, TRICARE Prime and TRICARE Program: Financial Management; 10 USC 1079, Contracts for Medical Care for Spouses and Children: Plans; 10 USC 1079a, TRICARE Program: Treatment of

Refunds and Other Amounts Collected Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); 10 USC 1086, Contracts for Health Benefits for Certain Members, Former Members, and Their Dependents; 10 USC 1095, Health Care Services Incurred on behalf of Covered Beneficiaries: Collection From Third-party Payers; 42 USC 290dd, Substance Abuse Among Government and Other Employees; 42 USC 290dd-2, Confidentiality Of Records; 42 USC 42 USC Ch 117, Sections 11131-11152, Reporting of Information; 45 CFR 164, Security and Privacy; DoD Instruction 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFS); DoD 6025.18-R, DoD Health Information Privacy Regulation; 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.

System does not collect information from the public. This is only DoD beneficiary data with potential to collect information on foreign nation friendly and enemy personnel who are treated in deployed US MIL treatment facilities.