



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Medical Operational Data System (MODS)

US Army Medical Command - Defense Health Program (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.

A0040-66b DASG:

10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 1071-1085, Medical and Dental Care; 50 U.S.C. Supplement IV, Appendix 454, as amended, Persons liable for training and service; 42 U.S.C. Chapter 117, Sections 11131-11152, Reporting of Information; 10 U.S.C. 1097a and 1097b TRICARE Prime and TRICARE Program; 10 U.S.C. 1079, Contracts for Medical Care for Spouses and Children; 10 U.S.C. 1079a, CHAMPUS; 10 U.S.C. 1086, Contracts for Health Benefits for Certain Members, Former Members, and Their Dependents; E.O. 9397 (SSN); DoD Instruction 6015.23, Delivery of Healthcare at Military Treatment Facilities (MTFs); DoD Directive 6040.37, Confidentiality of Medical Quality Assurance (QA) Records; DoD 6010.8-R, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); Army Regulation 40-66, Medical Record Administration and Health Care Documentation.

A0351a DASG:

10 U.S.C. 3013, Secretary of the Army; Army Regulation 351-3, Professional Education and Training Programs of the Army Medical Department; and E.O. 9397 (SSN).

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.

The Medical Operational Data System (MODS) provides the Office of The Surgeon General (OTSG), the US Army Medical Command (MEDCOM) staff, commanders, functional managers, and other stakeholders with an interactive and responsive worldwide operational system. MODS is a System-of-Systems (SoS) that provides over 100,000 users with tools and data needed to manage the Total Army medical readiness, medical manpower and personnel, medical logistics, medical education, operational support, and training during peacetime and mobilization. MODS is the Department of the Army Management Information System of Record for managing and integrating medical readiness data for individuals and organizations. In addition to managing readiness data, MODS supports the MEDCOM health readiness management needs by providing process-based web applications. MODS is an automation support tool in its operations and maintenance life-cycle mode with continued maintenance changes being performed as the medical community adjusts processes and requirements to support the global war on terrorism.

Currently, MODS has 44 active applications. They are as follows:

- Accepted List Positions (ALP)
- AMEDD Combat Zone Deployment History
- AMEDD Human Resources - Web Reporting (AWR)
- AMEDD Resource Tracking System
- Behavioral Health Data Portal (BHDP)
- Command Management System
- Contingency Battle Roster
- Continuing Medical Education
- Electronic Profile (eProfile)
- Emergency Medical Services (EMS)
- Enterprise Survey System
- Foreign Affiliate
- Health Care Specialist Tracking System (68W)
- Homeland Support Missions
- Human Capital Distribution Plan
- Medical Education Administration
- Medical Education Budget
- Medical Education Health Professions Loan Repayment Program (HPLRP)
- Medical Education Health Professions Scholarship Program (HPSP)
- Medical Education First Year Graduate Medical Education (FYGME)
- Medical Education Graduate Medical Education (GME)
- Medical Health Assessment (MHA)
- Medical Material Mobilization Planning Tool
- Medical Protection System (MEDPROS)
- Medical Protection System (MEDPROS) Web Data Entry
- Non-Deployable Report
- Obligation Worksheet Reporting
- Periodic Health Assessment
- Personnel Administration Division
- Personnel Deployment System Battle Roster
- Professional Filler System (PROFIS) Decision Support Tool
- Professional Filler System (PROFIS) Replacement Tracking
- Professional Filler System (PROFIS) Web Reporting (Web)
- Situation Report
- Soldier Patient Locator
- Soldier Patient Tracking
- Special Pay Module
- Special Forces Medical Sergeant (18D)
- Store and Forward
- Traumatic Brain Injury Tracker (TBI-T)

- User Management
- Volunteer
- Volunteer Management
- Warrior Transition
- 90 Day Boots on Ground Rotation (Web)

Categories of individuals with records in MODS include:

- Military members of the Armed Forces (both active and inactive)
- Retired Armed Forces personnel
- Family members
- DoD civilian employees
- DoD civilian retirees
- DoD contractors
- Foreign Nationals

Categories of Users include:

- Personnel who complete the pre/post deployment health assessment online forms
- Personnel who manage an application hosted by MODS
- Leaders who manage personnel via MODS applications

The types of PII collected include: Demographic data; spouse and child information; medical information; disability information; security clearance; emergency contact; employment information; military records; and education information.

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

Risks include unauthorized access to PII, inaccurate information in the system, and unauthorized disclosure of PII. There are administrative, physical, and technical security safeguards in place to mitigate these risks. The specific security safeguards are addressed in Section 3 below.

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.

Army Program Executive Office - Enterprise Information Systems (PEO-AIS)
 Combined Arms Center - Training, Collective Training Dir. (CAC-T, CTD)
 Deputy Chief of Staff, Army G-1
 Deputy Chief of Staff, Army G-3/5/7 (DAMO-ODR)
 Office of the Army CIO/G-6
 Office of the Surgeon General (OTSG) Decision Support Center (DSC)
 U.S. Army Aeromedical Center (USAAMC)
 U.S. Army Cadet Command (USACC)
 U.S. Army Dental Command (DENCOM)
 U.S. Army Forces Command (FORSCOM)
 U.S. Army Human Resource Command (HRC)
 U.S. Army Material Command (AMC)

U.S. Army Reserves Command (USARC)
U.S. Medical Command (MEDCOM)
Army National Guard

Other DoD Components.

Specify. US Air Force Medical Support Agency (AFMSA)
Armed Forces Health Surveillance Center (AFHSC)
Defense Finance and Accounting Service (DFAS)
Defense Health Information Management System (DHIMS)
Defense Health Services Systems (DHSS)
Reserve Health Readiness Program (RHRP)

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify. CentreLearn
Swank HealthCare
Language in Contracts/Agreements for the two contractors above:
The contractor must operate within it own secure datacenter in compliance with DoD Security and Privacy regulations, as required. Access to privacy data is restricted to only authorized and proper data access controls, as authorized by the contractor and the data owner.

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.

Individuals who complete the online DoD pre/post deployment health assessment forms have the opportunity to object to the collection of their PII. A Privacy Act Statement is prominently displayed on these forms. If the individual does not provide their PII, comprehensive healthcare services may not be possible or administrative delays may occur. HOWEVER, CARE WILL NOT BE DENIED.

(2) If "No," state the reason why individuals cannot object.

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.

Individuals who complete the online DoD pre/post deployment health assessment forms have the opportunity to object to the collection of their PII. A Privacy Act Statement is prominently displayed on these forms. If the individual does agree with the specific uses of their PII, comprehensive healthcare services may not be possible or administrative delays may occur. **HOWEVER, CARE WILL NOT BE DENIED.**

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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 Privacy Act Statement provided below is displayed on the following forms:
-DD Form 2795 Pre-Deployment Health Assessment
-DD Form 2796 Post-Deployment Health Assessment (PDHA)
-DD Form 2900 Post-Deployment Health Re-Assessment (PDHRA)

PRIVACY ACT STATEMENT
AUTHORITY: 10 U.S.C. 136, Under Secretary of Defense for the Personnel Readiness; 10 U.S.C. 1074f, Medical Tracking System for Members Deployed Overseas; 45 CFR Parts 160 and 164, Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules; and E.O. 9397 (SSN), as amended.

PURPOSE:To obtain information from and individual in order to assess the state of the individual's health before possible deployment outside the United States, its territories and its possessions as part of a contingency, combat, or other operation and to assist health care providers in identifying and providing present and future medical care to the individual. The information provided may result in a referral for additional health care that may include medical, dental, or behavioral health care or diverse community support services.

ROUTINE USES: In addition to those disclosures generally permitted under 5 U.S. 552a(b) of the

Privacy Act of 1974, as amended, the DoD "Blanket Routine uses" under 5 U.S.C. 552a(b)(3) apply to this collection. Information collected from you may be shared with other Federal and State agencies and civilian health care providers, as necessary, in order to provide necessary medical care and treatment and to guide possible referrals. For additional information see http://dpclo.defense.gov/privacy/SORN/blanket_routine_uses.html

DISCLOSURE: Voluntary. If you chose not to provide information, comprehensive healthcare services may not be possible or administrative delays may occur. HOWEVER, CARE WILL NOT BE DENIED.

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.