



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Medical Operational Data System (MODS)

US Army Medical Command - 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

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.

Statutory Authority: 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.

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) 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 readiness data, MODS supports the U.S. Army Medical Command health readiness management needs by providing process-based web applications. MODS is an automation support tool in its operations and maintenance lifecycle mode with continued maintenance changes being performed as the medical community adjusts processes and requirements to support the global war on terrorism. The PII collected includes: Demographic data; spouse and child information; medical information; disability information; security clearance; emergency contact; employment information; military records; emergency contact; 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. These risks are addressed by the following:

- 1) The system has role-based access controls.
- 2) MODS is pulling data from other systems (DEERS, etc). Information is matched via SSN. If there is not a match, data is not used.
- 3) Appropriate safeguards are in place to minimize the possibility of disclosure. The database is physically housed in an access-controlled server room and appropriate application level security is in effect.

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)

Other DoD Components.

Specify.

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)
National Guard Bureau (NGB)
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 have the opportunity to object to the collection of data during the use of the system or in the appropriate approved DoD form where data is collected. The system prominently displays the system Privacy Act Statement and Privacy and Security notices in accordance with the law and DoD policy.

(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 have the opportunity to consent to the specific uses of their PII on the appropriate DD or standard forms in electronic form or in paper. The system prominently displays the system Privacy Act Statement and Privacy and Security notices in accordance with the law and DoD policy.

(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.

PRIVACY ACT STATEMENT
The Privacy Act Statements are provided on the each of the forms associated with MODS.

PRIVACY AND SECURITY NOTICE
This site is provided as a public service by the Army Medical Department. This site is intended to be used for viewing and retrieving information only. Unauthorized attempts to change information on this service or tamper with this web site are strictly prohibited and may be punishable under the Computer Fraud Act of 1986 and the National Information Infrastructure Protection Act.
All information, including personal information, placed on or sent over this system may be monitored. Statistics and other information about your visit may be recorded. Use of this system constitutes consent to monitoring for these purposes.
For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.
Cookie Disclaimer - This Website does not use persistent cookies (persistent tokens that pass information back and forth from the client machine to the server). This site may use session cookies (tokens that remain active only until you close your browser) in order to make the site easier to use. This web site DOES NOT keep a database of information obtained from these cookies.
You can choose not to accept these cookies and still use the site, but it may take you longer to fill out the same information repeatedly and clicking on the banners will not take you to the correct link. Refer to the help information in your browser software for instructions on how to disable cookies.

PRIVACY ACT WARNING
(Applies to any system accessed by this connection which contains individual data subject to protection by the Privacy Act of 1974)
Personally Identifiable Information contained in this system is subject to the 5 U.S.C. 552a, as amended, the Privacy Act of 1974 and DoD 5400.11-R, "Department of Defense Privacy Program."
Personally Identifiable Information contained in this system may be used only by authorized persons in the conduct of official business. Any individual responsible for unauthorized disclosure or misuse of

personal information may be subject to a fine of up to \$5000. Executive Order 9397 authorizes solicitation and use of social security numbers (SSN's) as a numerical identifier for federal personnel that are identified in most federal record systems.

HIPAA WARNING

(Applies to any system accessed by this connection which contains data related to the health of an individual)

Protected Health Information in this system is subject to Public Law 104-191, the Health Insurance Portability and Accountability Act of 1996 and the Final Privacy Rule and Final Security Rule codified in 45 C.F.R. § 160 and 164, DoD 6025.18-R, "DoD Health Information Privacy Regulation" and DoD 8580.02-R, "DoD Health Information Security Regulation." Information in this system may only be used and/or disclosed in strict conformance with these authorities. The US Army Medical Command is required to, and will apply, appropriate sanctions against individuals who fail to comply with its privacy policies and procedures.

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.