



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Protocol Management System (PROMAS)

US Army Medical Command - Defense Health Program (DHP) Funded Application

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.

10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 32 CFR 219, Protection of Human Subjects; DoD Directive 5136.01, Assistant Secretary of Defense for Health Affairs (ASD(HA)); DoDI 3216.01, Use of Animals in DoD Programs; and DoDI 3216.02, Protection of Human Subjects and Adherence to Ethical Standards in DoD Supported Research.

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.

Protocol Management System (PROMAS) is a locally developed database system used within the Western Region Medical Command entities performing research. PROMAS documents the review process, training and qualifications of those federal employees, contractors, and civilians conducting and reviewing research. This information is needed to perform the Department of Clinical Investigation (DCI) mission of oversight of research projects throughout the region. Locally entered data is combined with Electronic Institutional Review Board (EIRB) system data via raw data reports to accomplish mission tasks such as generating metrics and research reports for department chiefs.

The PII collected and stored are name, employee information, education information, and trainee category (staff, resident, fellow, student, and other).

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

The risks associated with the collection, use, and storage of PII are unauthorized access and unauthorized disclosure. Loss or compromise could occur through insecure or misdirected digital transmission, insecure storage (data-at-rest), or loss of printed copy. Technical, administrative, and physical safeguards are in place to minimize these risks as indicated in Section 3d and 3f 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.

The PII is shared with personnel assigned to the Western Region Medical Command, Office of Research Protections, US Army Medical Research and Materiel Command; US Army Clinical Investigation Programs at the medical treatment facilities, and the US Army Human Research Protections Office.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

The PII is shared with authorized personnel within the US Food & Drug Administration and Department of Health and Human Services, Office of Human Research Protections if required.

State and Local Agencies.

Specify.

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

Specify.

The PII is shared with required and authorized personnel within the following agencies: The Geneva Foundation, Henry M. Jackson Foundation for the Advancement of Military Medicine, and Lovelace Respiratory Research Institute. Their contracts require compliance with the Privacy Act and Health Insurance Portability and Accountability Act (HIPAA) requirements to protect the confidentiality of personal information.

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

Specify.

The PII is shared with the researchers who have been established as collaborators under a Cooperative Research and Development Agreement.

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.

The PII for this electronic collection is not collected directly from the individual. The PII is collected from required documents submitted to the Department of Clinical Investigation (DCI) for approval to perform research.

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.

The PII for this electronic collection is not collected directly from the individual. The PII is collected from required documents submitted to Department of Clinical Investigation (DCI) for approval to perform research.

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 PII for this electronic collection is not collected directly from the individual. The PII is collected from required documents submitted to Department of Clinical Investigation (DCI) for approval to perform research.

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.