



PRIVACY IMPACT ASSESSMENT (PIA)

For the

MeRITS - MEDICAL RESEARCH INFORMATION TECHNOLOGY SYSTEM

US Army Medical Command

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. 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; 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 Research Information Technology System (MeRITS) is located at the US Army Medical Research & Materiel Command (USAMRMC) . It provides the command with a suite of information technology (IT) capabilities that comply with the US Food and Drug Administration (FDA) standards for Electronic Records and Electronic Signatures. MeRITS supports the medical research activities and makes it possible for USAMRMC to perform its core mission activities with the FDA.

MeRITS consist of the following:

- Electronic Document Management System (EDMS) provides electronic document management capability for FDA regulated and Research Management Enterprise non-regulated activities across USAMRMC. EDMS provides a centralized coordination/collaboration capability for approximately 500 users worldwide within the medical research community; usage is forecasted to increase month-to-month.
- Serious Adverse Event (SAE) provides electronic storage and automation for serious adverse event management/reporting. SAE usage is localized within the US Army Medical Materiel Development Agency Safety Division.
- Electronic Data Capture-Clinical Research Data Management System (EDC-CRDMS) provides the capability to electronically manage clinical trial data in support of medical research activity across USAMRMC. The system supports the full life cycle of clinical studies from study inception, through data field definition/specification, data entry, data query, data transfer/output into stand-alone statistical tools, and study close-out.
- Electronic Common Technical Document (eCTD) Publisher meets the FDA requirement to submit documentation in standard eCTD format. The eCTD interfaces with EDMS to pull documents from that system and compile them into an FDA acceptable format for all electronic submissions from USAMRMC.
- Clinical Trial Management System (CTMS) provides the ability to manage the overall clinical trial/study process. CTMS is a web based application that will meet the FDA regulations governing clinical trials with multiple groups and individuals completing the clinical trial/study tasks with minimum delays and maximum coordination.

The PII is collected from subjects where the clinical and medical trials are conducted to include medical treatment facilities (MTFs), research facilities, and from sponsor electronic regulatory files. Files containing PII are historical and are in a document form, where they are converted to electronic records when uploaded into the system. Other records collected are electronic, but these do not include social security numbers, addresses, and names. PII is populated in MeRITS by the user, and can only be uploaded and accessed by authorized users. The type of data retrieved from MeRITS includes that of medical and clinical trials.

The types of information collected include: Name, citizenship, race/ethnicity, mailing/home address, birth date, home telephone number, medical information, employment information, gender, place of birth, personal email address, and other information such as unique patient ID or identifier within the specific trial, patient count, age, and parent information.

This PIA replaces the MeRITS PIA approved on 10 October 2013.

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

The privacy risks associated with the PII collection are unauthorized access and unauthorized disclosure of PII. There are physical, technical, and administrative security safeguards in place to mitigate these risks. These security safeguards are addressed in Section 3 below.

[Empty box]

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 authorized health care providers, employees, and researchers, within the US Army Medical Treatment Facilities, US Army Medical Command Headquarters, and the US Army Medical Research and Materiel Command

Other DoD Components.

Specify.

The PII is shared with authorized personnel within the following: Air Force, Marines, Coast Guard, Air Force Medical Research Agencies; and Armed Forces Health Surveillance Centers.

Other Federal Agencies.

Specify.

[Empty box]

State and Local Agencies.

Specify.

[Empty box]

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

Specify.

Leidos Inc., GTI Federal Inc., Nanavanti Inc.
Language in contract for all contractors: The contractor may use or disclose Protected Health information on behalf, or to provide services to, the Government for treatment, payment, or healthcare operations purposes, in accordance with the specific use and disclosure provisions below, if such use or disclosure of Protected Health Information would not violate the HIPAA Privacy and Security Rule, DoD 6025.18-R or DoD 8580.02-R if done by the Government. The contractor may disclose Protected Health Information for the proper management and administration of the Contractor, provided that it will remain confidential and used or further disclosed only as required by law for the purpose for which it was disclosed to the person, and the person notifies the Contractor of any instances of which it is aware in which the confidentiality of the information has been breached. The contractor agrees to use administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits in the execution of this Contract.

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

Specify.

[Empty box]

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.

The individual is present at the time of PII collection and receives a Privacy Act Statement, DD Form 2005, for signature. This all inclusive Privacy Act Statement applies to all requests for personal information made by care treatment personnel and will become a permanent part of the health care record. If the individual

does not consent to providing the PII requested, he/she will not participate in the research study.

(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.

Department of Defense (DD) Form 2005, Privacy Act Statement – Health Care Records, is provided to the patient for review and signature. This all inclusive Privacy Act Statement applies to all requests for personal information made by care treatment personnel and will become a permanent part of the health care record. If individuals object to the specific uses of their PII, the individual will not take part in the research study.

(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.

DEPARTMENT OF DEFENSE (DD) FORM 2005, PRIVACY ACT STATEMENT – HEALTH CARE RECORDS, JUNE 2016
1. AUTHORITY FOR COLLECTION OF INFORMATION INCLUDING SOCIAL SECURITY NUMBER (SSN):

10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. Chapter 55, Medical and Dental Care; 42 U.S.C. Chapter 32, Third Party Liability for Hospital and Medical Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); DoDI 6055.05, Occupational and Environmental Health (OEH); and E.O. 9397 (SSN), as amended.

2. PRINCIPAL PURPOSES FOR WHICH INFORMATION IS INTENDED TO BE USED:

Information may be collected from you to provide and document your medical care; determine your eligibility for benefits and entitlements; adjudicate claims; determine whether a third party is responsible for the cost of Military Health System (MHS) provided healthcare and recover that cost; evaluate your fitness for duty and medical concerns which may have resulted from an occupational or environmental hazard; evaluate the MHS and its programs; and perform administrative tasks related to MHS operations and personnel readiness.

3. ROUTINE USES:

Information in your records may be disclosed to:

- Private physicians and Federal agencies, including the Department of Veterans Affairs, Health and Human Services, and Homeland Security (with regard to members of the Coast Guard), in connection with your medical care;
 - Government agencies to determine your eligibility for benefits and entitlements;
 - Government and nongovernment third parties to recover the cost of MHS provided care;
 - Public health authorities to document and review occupational and environmental exposure data;
- and
- Government and nongovernment organizations to perform DoD-approved research.

Information in your records may be used for other lawful reasons which may include teaching, compiling statistical data, and evaluating the care rendered. Use and disclosure of your records outside of DoD may also occur in accordance with 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, which incorporates the DoD Blanket Routine Uses published at:

<http://dpclid.defense.gov/privacy/SORNsIndex/BlanketRoutineUses.aspx>.

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 by DoD 6025.18-R. Permitted uses and disclosures of PHI include, but are not limited to, treatment, payment, and healthcare operations.

4. WHETHER DISCLOSURE IS MANDATORY OR VOLUNTARY AND EFFECT ON INDIVIDUAL OF NOT PROVIDING INFORMATION:

Voluntary. If you choose not to provide the requested information, comprehensive health care services may not be possible, you may experience administrative delays, and you may be rejected for service or an assignment. However, care will not be denied.

This all inclusive Privacy Act Statement will apply to all requests for personal information made by MHS health care treatment personnel or for medical/dental treatment purposes and is intended to become a permanent part of your health care record.

Your signature merely acknowledges that you have been advised of the foregoing. If requested, a copy of this form will be furnished to you.

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.