



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Enterprise Information Technology Service Management Solutions
(Remedy, E-Talk, and Kinetic Request)

US Army Medical Command - DHP Funded Applications

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.

DMDC 02 DoD:

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. Chapters 53, Miscellaneous Right and Benefits, Chapter 54, Commissary and Exchange Benefits, Chapter 55 Medical and Dental Care, Chapter 58 Benefits and Services for Members being Separated or Recently Separated, and Chapter 75 Deceased Personnel; 10 U.S.C. 136 Under Secretary of Defense for Personnel Readiness; 20 U.S.C. 1070a (f)(4), Higher Education Opportunity Act; 31 U.S.C. 3512(c) Executive Agency Accounting and Other Financial Management; 50 U.S.C. Chapter 23, Internal Security; DoD Directive 1341.1, Defense Enrollment/Eligibility Reporting System; DoD Instruction 1341.2, DEERS Procedures; 5 U.S.C. App. 3 (Pub.L. 95-452, as amended Inspector General Act of 1978; Pub.L. 106-265, Federal Long-Term Care

Insurance; and 10 U.S.C. 2358, Research and Development Projects; 42 U.S.C., Chapter 20, Subchapter I-G, Registration and Voting by Absent Uniformed Services Voters and Overseas Voters in Elections for Federal Office, Sec. 1973ff, Federal responsibilities and DoD Directive 1000.4, Federal Voting Assistance Program (FVAP); Homeland Security Presidential Directive 12, Policy for a common Identification Standard for Federal Employees and Contractors; 38 CFR part 9.20, Traumatic injury protection, Servicemembers' Group Life Insurance and Veterans' Group Life Insurance; 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.

This PIA addresses three Enterprise Information Technology (IT) Service Management Solutions. They are as follows:

1) Remedy IT Service Management System is a enterprise-wide tool for managing IT services. It reduces complexity and makes customer support, change, asset, and request management a seamless integrated process. When an IT system fails or needs maintenance, a trouble ticket is created in the Remedy system and assigned to a technician for action. Remedy collects and stores information about IT users and support staff to include name, rank/grade, work address, work E-mail address, and work telephone number. Any required medical data will be collected from the health care provider, not the actual patient, for the purposes of verifying or correcting medical records.

2) E-Talk system is a quality control telephone call recording solution. This system records all in/out bound telephone calls related to IT support issues at medical treatment facilities (MTF). Customers may report issues with medical records or be required to provide the last four digits of their social security number for identification verification which is tracked in the Remedy system mentioned above.

3) Kinetic Request provides a user intuitive web interface for end-users to submit IT related trouble tickets or requests for service. The customizable interface allows IT personnel to build an environment that will guide the user through the trouble ticket creation process. This will be accomplished by gathering required information, suggesting self-help fixes, and even automatically assigning the request to the correct support group based on the answers received.

The types of personal information collected include demographic data, employment information, and medical information.

(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 collected are unauthorized access, inaccurate information entered into the application, and unauthorized disclosure of PII. Security safeguards are in place to mitigate these risks.

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. PII is shared with personnel within the US Army Medical Information Technology Center (USAMITC).

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

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

Specify. Some individuals who administer these applications are employed on a contractual basis. There are clauses in their contracts requiring 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.

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 individual does not directly participate in the PII collection process. PII is obtained from existing DoD systems.

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 individual does not directly participate in the PII collection process. PII is obtained from existing DoD systems.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|---|--|
| <input type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input checked="" type="checkbox"/> None |

Describe each applicable format.

The individual does not directly participate in the PII collection process. PII is obtained from existing DoD systems.

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.