



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Document & Referral Management System (DRMS)
--

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.

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 purpose of this system is to provide a real-time, transparent view of shared patient data and documents to personnel at both Tripler Army Medical Center (TAMC) and the Veterans Affairs Pacific Island Health Care System (VAPIHCS) who need the information in support of referral and authorization management, continuity of care, billing and payment, and tracking and forecasting. This information historically has been located in one agency's legacy system which made it difficult, if not impossible, to share the information with the other agency. Personal information includes: Name, Citizenship, Race/Ethnicity, Mailing/Home Address, Marital Status, Birth Date, Home Telephone Number, Religious Preference, Medical Information, Employment Information, Social Security Number (SSN), Gender, Spouse Information, and Military Records.

(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 will have role-based access;
- 2) DRMS is pulling data from other systems and the 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.

**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.

The following verbiage is inserted in the contract related to the safeguarding of PII:

1) The contractor/subcontractor must provide security in order to control and manage access to specific types of bills and data.

- 2) The contractor is responsible for providing signed business associate agreements for all personnel prior to beginning the work on this task order.
- 3) The contractor shall protect against unauthorized disclosure of data to ensure the privacy of Government contractors and private individuals for which the information is maintained. All data maintained by the contractor's solution is subject to the provisions of the Privacy Act of 1974; DoD 5400.11-R, DoD Privacy Program; and DoD 5200.11-R, DoD Information Security Program. Additionally, data falls within the content of Exemption Numbers 3, 4 and 6 of DoD Freedom of Information Act (FOIA) program. Each of these programs mandates adequate control and protection of sensitive data. The contractor shall ensure that the application meets the features of identification and authentication, auditing, and discretionary access control. Additionally, the contractor will employ Federal Information Processing Standards (FIPS) 140-1 compliant encryptions and digital certificates for web based components.
- 4) This task is UNCLASSIFIED. However if the performance of this contract requires access to personal identifiable data the contractor shall comply with the requirements of the Privacy Act of 1974. The contractor shall retain in strictest confidence and prevent the unauthorized duplication, use and disclosure of identifying information. This data shall only be used for the designated contract and tasks. Files (electronic and written) of data requests shall be maintained in accordance with appropriate guidelines provided by the contract officer and applicable regulations.
- a) The contractor shall use personnel information for their designated contract tasks. This information shall not be used to create data bases or any other project not intended for use specifically for the project. All personnel information related to this contract shall be destroyed at the conclusion of the contract.
- b) The contractor shall maintain, transmit and retain in strictest confidence all personal identifiable information, as well as prevent the unauthorized duplication, use, and disclosure of such data. The contractor shall provide personnel information only to employees having a need to know such information in the performance of their duties for this contract.
- c) Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only" The contractor shall comply with Resource Management Office memorandum, Acquisition Document Security Markings, February 15, 1994.
- d) The contractor will not require access to classified data.
- e) Due to continuing concerns for the security and privacy of information in health care settings the Government has established requirement for the conduct of security practice and Data Use Agreements (DUA) in the information management and information systems development process. Appendix C provides the specific documentation requirements that will need to be met to assure security and compliance.
- 5) All data received, processed, evaluated, loaded and/or created as a result of this contract shall remain the sole property of TAMC.
- 6) The contractor shall incorporate all applicable laws and regulations governing healthcare information and information systems, including Health Insurance Portability and Accountability Act (HIPAA) requirements, the Rehabilitation Act and the Americans with Disabilities Act.

**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 participate in the data collection process.

**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.

The individual does not participate in the data collection process.

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

The individual does not participate in the data collection process.

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 individual does not participate in the data collection process

**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.