



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Search and Data Aggregation System (Softek Illuminate®)

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
- 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.

Softtek Illuminate® provides radiologists, pathologists and other clinicians, as well as educators and administrators, with the ability to instantly access the specific information they need. Driven by its patented vendor-neutral search technology, Illuminate® breaks down the information silos across hospital data systems to deliver a more complete picture – both current and historical - of the patients and the practice. Illuminate® helps improve productivity, clinical decision making and, ultimately, the quality of patient care. This PIA addresses the following Illuminate applications:

- InSight™. The intuitive search engine at the core of InSight™ delivers any radiology, pathology or lab report or group of reports in the organization's archive to use for clinical analytics, chronic disease tracking, research and education.

- PatientView™. PatientView automatically retrieves and displays all of a patient's relevant clinical history, including clinical notes, at the point of read to improve decision making and help to deliver actionable reports.

- Analytics™. Analytics delivers easy-to-use performance metrics. It delivers information in graphical formats that can be easily navigated, filtered and manipulated. It will be utilized by designated radiology personnel to monitor and track analytical information about the department such as productivity, utilization, and referring physicians.

- ActKnowledge™. ActKnowledge makes it easy to track the surveillance and follow-up treatment of at-risk patients – whether they are suffering from chronic diseases or have just been diagnosed with an incidental or critical finding.

The following personal identifying information is collected in the system: patient name, gender, date of birth, a unique patient identification number, and medical information specific to the system.

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

Risks for this system are similar to any other system which requires human data entry or are electronically accessible. These include unauthorized access, inadvertent data viewing, and unauthorized disclosure of PII. Risks are mitigated by strict adherence to security and privacy protocols. Physical, technical, and administrative safeguards are employed as indicated in Section 3 below. This multi-faceted approach to safeguarding PII provides redundant protections to both the PII and the institutions involved in the collection and management of this highly personal and sensitive information.

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 will be shared with health care providers within all US Army medical treatment facilities (MTF) using this application.

Other DoD Components.

Specify. The PII may be shared with health care providers within US Navy and US Air Force MTFs.

Other Federal Agencies.

Specify. The data may be shared with required and authorized health care providers within other Federal Agencies supporting the US Army and/or DoD beneficiaries (U.S. Coast Guard, Veterans Administration, Public Health Service, Center for Disease Control).

State and Local Agencies.

Specify.

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

Specify. If this product is purchased, the service contract will include the standard Military Health System (MHS) HIPAA Business Associate Agreement language and the US Army Medical Command Information Assurance (IA) requirements. The contractor will agree to use the administrative, physical, and technical security safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the protected health information it creates, receives, maintains, or transmits in the execution of the contract.

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.

This system is not the initial collection point for the PII. The PII is obtained from an existing system.

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.

This system is not the initial collection point for the PII. The PII is obtained from an existing system.

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.

This system is not the initial collection point for the PII; therefore, a Privacy Act Statement is not required.

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.