



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Teledermatology

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
- 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.

5 U.S.C. 301, Department Regulation; 10 U.S.C., Chapter 55; Pub.L. 104-91, Health Insurance Portability and Accountability Act of 1996; DoD 6025. 18-R, DoD Health Information Privacy Regulation; 10 U.S.C. 1071-1085, Medical and Dental Care; 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, Civilian Health and Medical Program of the Uniformed Services (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 6010.8-R, CHAMPUS; 10 U.S.C. 1095, Collection from Third Party Payers Act; 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.

The purpose of the teledermatology system is to provide an improved dermatology clinical process using a proven web based methodology to capture patient demographics, previous treatments, and images of the dermatology condition. It improves access to dermatology care and reduces the overall cost of network referrals for dermatology consultations. The patient benefits from improved access and a higher level of care. Providers are empowered with dermatology knowledge and are able to provide higher quality of care to their patients. The organization is able to more efficiently utilize our limited resources to reduce health care costs.

Teledermatology collects and maintains PII that includes Name, Social Security Number, Gender, Race/Ethnicity, Home telephone number, Medical Information, Age, Family Member Program category, Branch of Military Service, Military Status, and Patient Identifying Images (facial images and tattoos birthmarks, etc).

(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 has role-based access.
- 2) The system has no external connections with other systems and does not transfer data to any other system.
- 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.
- 4) Each teleconsultation is assigned a unique control number that is used to identify a specific consult. The patient's provider must log into the teledermatology system and enter the consultation control number to locate the patient record and associated PII.
- 5) The teledermatology server is protected by a proxy server to limit direct access to the web server.

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. Users at Army medical treatment facilities who are registered users in the teledermatology program are authorized to have access. The information is not shared through data exchange.

Other DoD Components.

Specify. Users at Navy and Air Force medical treatment facilities who are registered users in the teledermatology program are the only persons authorized to have access. The information is not shared through data exchange.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

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

Specify.

CNI Administration Services, LLC. The Contractor agrees to not use or further disclose Protected Health Information other than as permitted or required by the Contract or as Required by Law. The Contractor agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Contract. The Contractor agrees to implement 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 on behalf of the Government. The Contractor agrees to mitigate, to the extent practicable, any harmful effect that is known to the Contractor of a use or disclosure of Protected Health Information by the Contractor in violation of the requirements of this Contract. The Contractor agrees to report to the Government any use or disclosure of the Protected Health Information not provided for by this Contract. The Contractor agrees to report to the Government any security incident of which it becomes aware. The Contractor agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information, in any format, that it creates, receives, maintains, or transmits on behalf of the Government, agrees to the same restrictions and conditions that apply through this Contract to the Contractor with respect to such information. The Contractor agrees to provide access, at the request of the Government, and in the time and manner designated by the Government to Protected Health Information in a Designated Record Set, to the Government or, as directed by the Government, to an Individual in order to meet the requirements under 45 CFR 164.524. The Contractor agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Government directs or agrees to pursuant to 45 CFR 164.526 at the request of the Government or an Individual, and in the time and manner designated by the Government. The Contractor agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by the Contractor on behalf of, the Government, available to the Government, or at the request of the Government to the Secretary, in a time and manner designated by the Government or the Secretary, for purposes of the Secretary determining the Government's compliance with the Privacy Rule. The Contractor agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for the Government to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528. The Contractor agrees to provide to the Government or an Individual, in time and manner designated by the Government, information collected in accordance with this Clause of the Contract, to permit the Government to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

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.

Patients must sign a Consent Form (Authorization to Receive Telemedicine Services) before their PII can be placed into the teledermatology system. This form is used for multiple telemedicine consultations including store and forward as well as video teleconference consultations and is maintained by the medical treatment facility as part of the local medical record. Patients may refuse to participate in the teledermatology program which could delay their access to dermatology care.

(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.

Patients must sign a Consent Form (Authorization to receive Telemedicine Services) before their PII can be placed into the teledermatology system. This form is maintained by the medical treatment facility as part of the local medical record.

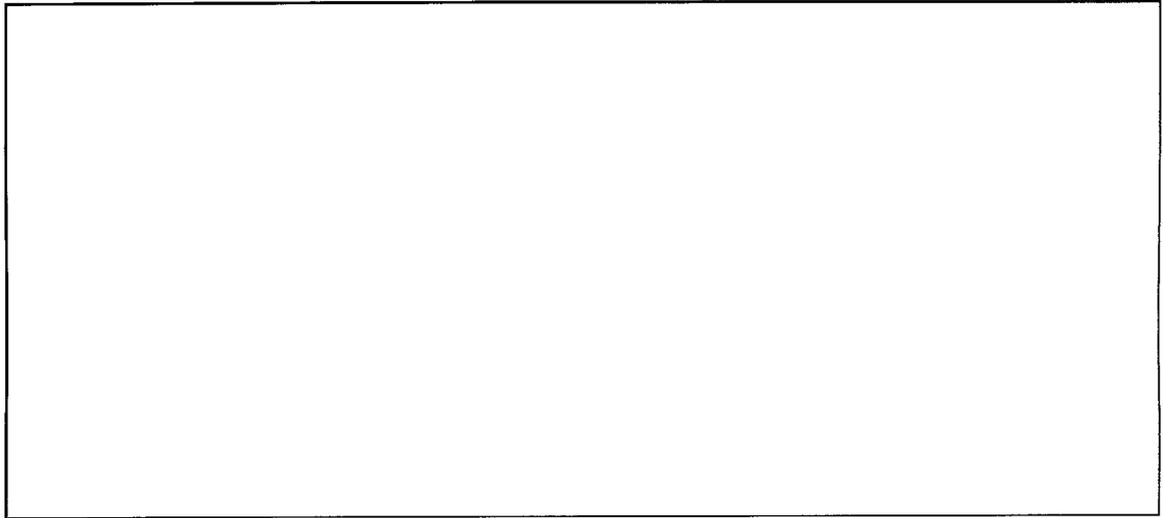
(2) If "No," state the reason why individuals cannot give or withhold their consent.

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.

Patients must sign a Consent Form (Authorization to Receive Telemedicine Services) before their PII can be placed into the teledermatology system.



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.