



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Army Medicine Secure Messaging Service (AMSMS)

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

A0040-66b DASG

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, as amended (SSN); DoD Instruction 6015.23, Delivery of Health care 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.

In 2008, The Army Surgeon General, in coordination with Health Affairs /TRICARE Management Activity (TMA), jointly agreed to a Military Health System-wide adoption of the Patient-Centered Medical Home (PCMH) Initiative. The PCMH workflows include high-level functional information management/information technology (IM/IT) requirements that now require IM/IT support, tool selection and implementation. In May 2011, the Office of The Surgeon General Chief Medical Information Office, in coordination with the US Navy Secure Messaging Executive Agent, began the acquisition of initial secure messaging licenses to pilot and field. This was prior to an US Army Medical Command (MEDCOM)-wide implementation of a fully developed, tested, and functional secure messaging capability between patients and health care providers. In Fiscal Year (FY) 2011, funding for 20 licenses was forwarded to the US Navy for use at the Army medical treatment facilities (MTF) at Fort Campbell, Kentucky, and Fort Bragg, North Carolina. These licenses were provided by the US Navy as the lead agent for this initiative. The licenses at these clinics will be identical to the licenses being procured for US Navy clinics. As of 13 September 2011, a one year contract was awarded to Relay Health to provide these services. This contract includes the award of 1,986 licenses for the first year. Additional licenses are being purchased for a pilot phase. This will expand the capability beyond that of the US Navy, and will provide Integrated Clinical Data Base-driven patient health record information for the patient via secure messaging (currently provided by the US Air Force). At the core of the MEDCOM PCMH Initiative is the need to improve communication between the primary care team and patient. The clinical workflows supporting PCMH are complete and will be used to identify how technologies (such as Web Portal, Secure Messaging, and Mobile Technology) are integrated and developed to create a single interface for the health care beneficiary, while being able to introduce follow-on services and sites.

The types of personal information collected include patient demographic data 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 by provider to patient and provider to provider within the Army MTFs using this application.

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.

1) The following contract language pertains to the Patient-Centered Medical Home Secure Messaging (PCMH-SM) contractors. The contractor for PCMH-SM is Relay Health:

7.1 Physical Security Requirements:

7.1.1 The contractor shall be responsible for safekeeping all project property utilized under this PWS. The vendor shall keep all facilities, equipment, and supplies secure each day. The contractor shall provide physical security for the servers on which the DoD patient information resides and must submit to and pass inspection by DoD personnel.

7.2 Information Assurance (IA):

7.2.1 The contractor vendor shall provide a report covering the current status of their system IA posture, in accordance with SECNAVINST 5239.3B and 45 C.F.R Parts 160 and 164, including but not limited to the following:

7.2.1.1 The contractor shall provide spam blocking to protect all users of the system from spam and other malware.

7.2.1.2 The contractor shall provide for cyber security of the servers to prevent hacking and other potential cyber-attacks on the data of DoD personnel. This must pass all HIPAA guidelines for PHI security.

7.2.1.3 The contractor shall provide a robust anti-malware solution to protect all end users from infection (i.e. viruses, key loggers, spyware, etc).

7.2.1.4 The system shall be fully HIPAA compliant and be at least 128 bit encryption of data.

7.2.1.5 System C & A documentation

7.3. Protection of Patient Information

7.3.1. The contractor shall maintain, transmit, retain in strictest confidence, and prevent the unauthorized duplication, use, and disclosure of patient information in accordance with 45 C.F.R Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information, Final Rule, December 28, 2000 (effective April 14, 2001) and The Privacy Act of 1974. The vendor shall provide patient information only to employees, contractors, subcontractors, and Government personnel having a need to know such information in the performance of their duties for this project.

7.4. Compliance with DoD Privacy Regulations

7.4.1. The contractor shall comply with the most current version, and all future changes when released, of all Government and DoD privacy regulations and directives, the Privacy Act 5.U.S.C. 552a, and other applicable Service privacy instructions and regulations. In addition, the contractor shall comply with the most current version and all future changes when changes are released, of all relevant rules published in the Federal Registrar to implement the HIPAA of 1996. This shall include Standards for Privacy of Individually Identifiable Health Information, Final Rule, published December 28, 2000.

2) Some health care personnel who have access to the system/electronic collection 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.

The patient is provided a Privacy Act Statement during the registration process for the AMSMS. If the patient objects to the collection of PII, AMSMS enrollment is not completed and use is prohibited.

(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.

The patient is provided a Privacy Act Statement during the registration process for the AMSMS. If the patient objects to the specific uses of their PII, AMSMS enrollment is not completed and use is prohibited.

(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.

The following information is provided to the patient at the time of registration for the AMSMS.

Dear (PATIENT NAME HERE),

You may now reach us online through Army Medicine Secure Messaging Service, a secure messaging service with an integrated Personal Health Record (PHR). I encourage you to communicate with us directly about non-urgent healthcare needs. Select the link below to complete your registration.

In accordance with the Privacy Act of 1974 (Public Law 93-579), this notice informs you of the purpose of this authorization and how it will be used. Please read it carefully.

AUTHORITY: Public Law 104-191; E.O. 9397 (SSAN); DoD 6026. 18-R.

PRINCIPAL PURPOSE(S): This authorization allows the Military Health System to release an individual's protected health information to RelayHealth.

ROUTINE USES(S): Upon authorization from the individual, protected health information may be released to the individual for personal use, or to the individual or a third party for insurance, continued medical care, school, legal retirement/separation, or other reasons.

DISCLOSURE: Voluntary.

RELEASE AUTHORIZATION: I understand that:

a) I have the right to revoke this authorization at any time. My revocation must be in writing and provided to the local MTF or DTF.

b) If I authorize my protected health information to be disclosed to someone who is not required to comply with federal privacy protection regulations, then such information may be re-disclosed and would no longer be protected.

c) I have a right to inspect and receive a copy of my own protected health information to be used or disclosed, in accordance with the requirements of the federal privacy protection regulations found in the Privacy Act and 45 CFR 164.524.

Proceeding with the completion of the registration for this account implies authorization to release my Patient Health Record information to RelayHealth.

I request and authorize the Military Health System to release my Personal Health Records to RelayHealth.

Register now.

<https://app.relayhealth.com/Invite/PIMgr.aspx?token=21558252269B8B> <blocked<https://app.relayhealth.com/Invite/PIMgr.aspx?token=21558252269B8B>>

Click this link or paste it into your browser's address field.

If you have any difficulty registering or using the service please contact RelayHealth Customer Support at 1-866-RELAY-ME (1-866-735-2963) or by e-mail at support@relayhealth.com.

Learn more (take a tour).

<https://app.relayhealth.com//ResourceLibrary/rh/general/onlineQuicktour/html/PatientQuickTour.html>

<blockedhttps://app.relayhealth.com//ResourceLibrary/rh/general/onlineQuicktour/html/
PatientQuickTour.html>

NOTE: PLEASE DO NOT REPLY TO THIS INVITATION E-MAIL. REGISTER FOR THE SECURE SERVICE TO COMMUNICATE ONLINE WITH ME.

Sincerely,

PROVIDER NAME HERE

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.