



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Guest Network Account Solution (ClearPass Access Management System™)

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.

- DoDI 8500.1, Cybersecurity, 14 March 2014.

- AR 25-2, Information Assurance, RAR Date: 23 March 2009.

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 Aruba Networks ClearPass Policy Manager™ platform provides role-based and device-based network access control for US Army Medical Command (MEDCOM) guests across the wireless infrastructure. The account registration website and internet access are provided as a public service for beneficiaries and guests physically located at MEDCOM medical treatment facilities (MTFS). Categories of guests include patients, family members, visitors and vendors. ClearPass supports self-service registration capabilities for these guests. Its customizable captive portal capabilities allow the creation of a branded guest login experience with code-of-conduct messaging and delivery/acceptance of the Acceptable Use Policy. The ClearPass Authentication Appliance collects the users first name, last name, email address, and media access control address (MAC address) during registration. The system generates an account and emails the user name and password to the user. The user information is stored in a database on the ClearPass server for user authentication only, and is flushed within 24 hours. The logs from the ClearPass are sent to a Security Event and Incident Management (SEIM) server for log correlation and security event management. These logs are only available to system administrators with the required need to know and appropriate privileges.

(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 collection are unauthorized access and unauthorized disclosure of PII. There are physical, technical, and administrative security safeguards in place to mitigate these risks. These safeguards are addressed in Section 3 below.

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.

- System Administrators within the DHA Network Operations Center using this application.
- Computer Network Defense Service Provider (CNDSP) and the Army Computer Emergency Response Team (ACERT) should there be a breach or unauthorized activity

Other DoD Components.

Specify.

US Cyber Command (US CyberCom) should there be a breach or unauthorized activity.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

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

Specify.

Contracting Company: ActionNet. To meet Information Assurance (IA) requirements, the MEDCOM WLAN services are configured, operated, and sustained in accordance with specific public laws, regulations, and policies to prevent the unauthorized disclosure, manipulation, or deletion of patient health care data, protected health information (PHI), personally identifiable information (PII), administrative, or logistical data.

Contract service providers are working in a limited access environment and are responsible for compliance with Army Security Programs in accordance with Department of Defense (DoD) and Department of the Army (DA) Directives to include all security regulations and policies in effect at the work site such as Army Regulation's 190-12, 380-5, 25-1, 25-2.

Contract service providers shall be familiar with and adhere to the Privacy Act, Title 5 of the US Code, Section 552a and applicable agency rules and regulations.

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.

A Privacy Advisory is provided to the individual during the registration process. The opportunity to object is available at the initial point of the PII collection for the electronic collection. Consent is given by acceptance of the terms and conditions of the registration process. If individuals do not provide their PII, they will not be able to utilize the guest wireless services.

(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.

A Privacy Advisory is provided to the individual during the registration process. The opportunity to object to specific uses of the PII collected is available at the initial point of the PII collection. Consent to the specific

uses of their PII is given by acceptance of the terms and conditions of the registration process. If individuals withhold their consent and do not provide their PII, they will not be able to use the guest wireless services.

(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.

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

Describe each applicable format.

Privacy Advisory: This statement serves to inform you of the purpose for collecting personal information required by this system and how it will be used.

Authority: DoDI 8500.1, Cybersecurity, 14 March 2014.

PURPOSE: To collect information from personnel desiring to utilize Guest Wireless in order to authenticate users in accordance with Army Regulation 25-2 and DODI 8500.1.

ROUTINE USES: Use and disclosure of your records outside of DoD may occur in accordance with 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, which incorporates the DoD Blanket Routine Uses published at: <http://dpcl.d.defense.gov/Privacy/SORNSIndex/BlanketRoutineUses.aspx>

DISCLOSURE: Voluntary; however, failure to provide information may result in the denial of Guest Wireless Services.

This Web site provides registration for utilization of Guest Wireless services within this facility. The registration Website and Internet access are provided as a public service for beneficiaries and guests of US Army Medical Command Facilities.

For site security purposes and to ensure that this service remains available to all users, security systems are employed to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

Except for authorized law enforcement investigations and national security purposes, no other attempts are made to identify individual users or their usage habits beyond DoD websites. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration Guidelines. All data collection activities are in strict accordance with DoD Directive 5240.01.

Unauthorized attempts to upload information or change information on this site are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National

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.