



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Picture Archive and Communication System Integrator (PACSi)

Defense Health Information Management Systems (DHIMS)

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

DHA 07

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. Chapter 55, Medical and Dental Care; 32 CFR 199.17, TRICARE Program; and E.O. 9397 (SSN), as amended.

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 Picture Archiving and Communication System Integrator (PACSi) is a windows service oriented application and hardware solution that was initially piloted at William Beaumont Army Medical Center and the El Paso Veterans Affairs (VA) Health Care System. The project was developed to demonstrate and validate a bidirectional medical image sharing capability to leverage existing enterprise capabilities in both Department of Defense (DoD) / VA such as Digital Imaging Network - Picture Archiving and Communications System (DINPACS) and Veterans Health Information System and Technology Architecture (VistA) Imaging. This pilot project was eventually expanded to allow for the sharing of patient medical images and data between several Department of Veterans Affairs hospitals and six DoD Military Treatment Facilities (MTFs).

The patient images are shared utilizing the PACSi servers, the Bidirectional Health Information Exchange (BHIE) framework infrastructure, and the existing accredited Business to Business (B2B) Virtual Private Network (VPN) tunnel between DoD and VA.

The PACSi servers were procured by the VA as part of the pilot project. Currently, the DHIMS Product Management Office (PMO) is responsible for the maintenance and sustainment of this project.

The local PACSi server at the DoD MTFs provides the mechanism for communication and interface with the local Picture Archiving and Communications System (PACS) server at DoD MTFs. The PACSi also hosts the image viewing services for DoD users through the Medical Image Viewer (MIV). The PACSi Medical Image Viewer (MIV) application authenticates DoD users through the existing Composite Healthcare System (CHCS). DoD user credentials are managed by the accredited CHCS server. Existing CHCS login credentials (username/password) are used to provide access. VA users utilize their VistA system to acquire images from DoD MTFs. Once a patient image request is made by VA or DoD clinicians through a Medical Image Viewer connected to a PACSi server, the patient data and studies are returned from all PACSi-interconnected medical facilities where the patient has an existing record.

The PACSi servers can be equally accessed by DoD or VA Providers. The Interagency Image Sharing project is primarily used by the VA to access DoD images.

It is anticipated that this effort will be subsumed under the current Defense Health Information Management System (DHIMS) initiative entitled Health Artifact and Image Management System (HAIMS) that is being developed separately by the TRICARE Management Activity (TMA) under a separate development effort. Once HAIMS reaches initial operational capability and becomes the accepted DoD enterprise solution, this operations and sustainment project will be transitioned into that larger effort and will be discontinued as a separate operations effort.

The types of personally identifiable information (PII)/protected health information (PHI) that are stored within the PACSi servers include:

- Name (First/Last)
- Social Security Number (SSN)
- Other patient identification Number (FMP)
- Gender
- Birth date
- Medical information (radiology study)

The individuals whose PII / PHI is stored and transmitted within the system are individuals with active duty status as well as retired military service personnel.

The PII / PHI is shared between the six DoD MTF's and VA hospitals that participate in the Interagency Image Sharing project. The following is a list of the six (6) DoD facilities where the PACSi servers are located:

Walter Reed National Military Medical Center (WRNMMC), Bethesda, Maryland
William Beaumont Army Medical Center (WBAMC), El Paso, Texas
Evans Army Community Hospital (EACH), Colorado Springs, Colorado
Keesler Air Force Base (KEESLER), Biloxi, Mississippi
Naval Health Clinic Great Lakes (NHGL), Great Lakes, Illinois
Landstuhl Regional Medical Center (LRMC), Landstuhl, Germany

The PACSi servers are managed through a sustainment contract awarded by Defense Health Information Management System (DHIMS).

System Contact Information:

DHIMS
5111 Leesburg Pike
Skyline 5, Suite 817
Falls Church, Virginia 22041
(703) 681-7143
www.health.mil

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

Three potential privacy risks are associated with the PII / PHI transmitted and stored by the PACSi servers: 1) unauthorized access to the data/system, 2) inaccurate information contained in the system, and 3) unauthorized disclosure of PII/PHI from the system.

Safeguards are employed by the PACSi servers to detect and minimize unauthorized disclosure, modification, or destruction of data. Such safeguards include user authentication at logon to the system, access to data based on USERID while logged on, and tracking user modification of data. System log files record system use and login attempts (successful and otherwise).

No classified data is processed by the PACSi servers, and no classified data is communicated across the network. The information on the PACSi server includes PII/PHI that requires protection in accordance with the Privacy Act of 1974, as amended (Public Law 93-579) and controls in compliance with DoD 5400.7-R, "DoD Freedom of Information Act (FOIA) Program." Such information requires special handling, storage, safeguarding, marking, and disposal procedures as provided in DoD 5400.11-R, "DoD Privacy Program." The PACSi servers will support and comply with the appropriate DoD security requirements for encryption and compression of medical images transmitted over the network.

Remote access:

The System Administrators remotely access the server to apply patches through MHS Demilitarized Zone (DMZ) Remote Access Juniper Appliance. Remote access requires the system administrator to have a valid DoD Common Access Card (CAC).

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 / PHI is shared between the six (6) DoD Military Treatment Facilities and various VA hospitals that participate in the National Defense Authorization Act (NDAA) Interagency Image Sharing project. The following is a list of the six DoD facilities with PACSi servers:

Walter Reed National Military Medical Center (WRNMMC), Bethesda, Maryland
William Beaumont Army Medical Center (WBAMC), El Paso, Texas
Evans Army Community Hospital (EACH), Colorado Springs, Colorado
Keesler Air Force Base (KEESLER), Biloxi, Mississippi
Naval Health Clinic Great Lakes (NHCGL), Great Lakes, Illinois
Landstuhl Regional Medical Center (LRMC), Landstuhl, Germany

The PACS at each of the above locations provides the PII/PHI to their respective PACSi server co-located at each location.

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 contract with Evolvent Technologies contains a Business Associate Agreement (BAA) which states: "In accordance with DoD 6025.18-R "Department of Defense Health Information Privacy Regulation," January 24, 2003, the contractor meets the definition of Business Associate (BA). Therefore, a Business Associate Agreement is required to comply with both the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security regulations. This clause serves as that agreement whereby the Contractor agrees to abide by all applicable HIPAA Privacy and Security requirements regarding health information as defined in this clause, and in DoD 6025.18-R and DoD 8580.02-R, as amended."

Furthermore, the BAA states: "The Contractor agrees to use 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 in the execution of this 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.

Individuals cannot object because the collection of PII / PHI has already been done prior to any PII / PHI being accessed by the PACSi servers. The PACSi servers have a system-to-system interface with the local PACS that contains the stored PII / PHI.

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.

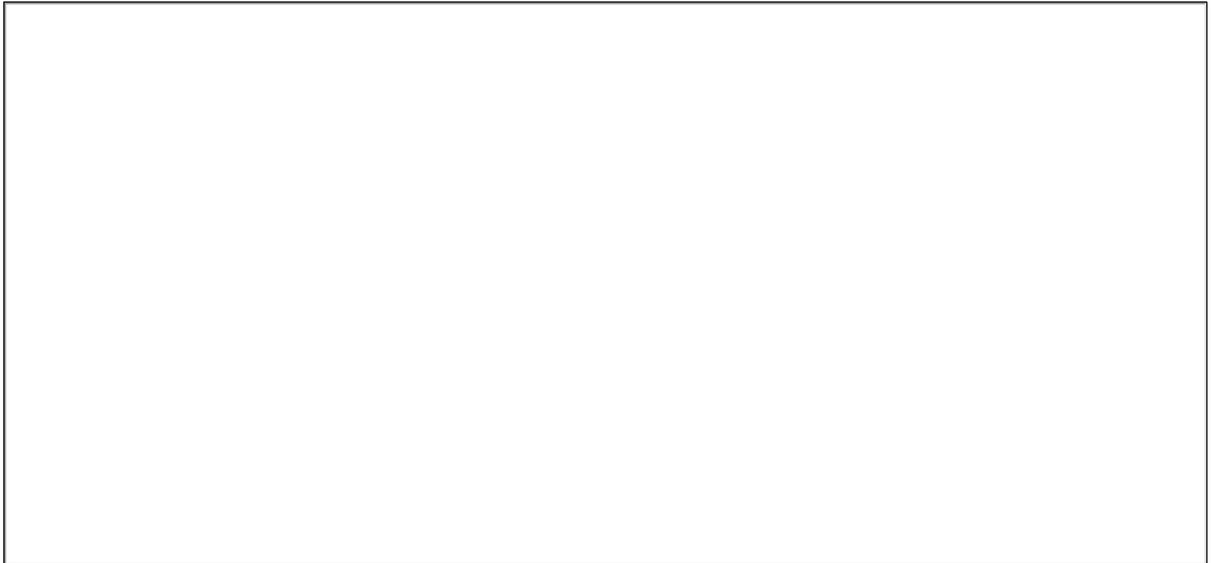
Individuals cannot object because the collection of PII / PHI has already been done prior to any PII / PHI being accessed by the PACSi servers. The PACSi servers have a system-to-system interface with the local PACS that contains the stored PII / PHI.

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.

Although PACSi is a system of records, it is not the initial point of collection for PII. Instead, all information sent through PACSi is acquired by PACS or another system that feeds into PACS. Accordingly, a Privacy Act Statement is not necessary.



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.