



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Deployed Tele-Radiology System (DTRS) / Theater Imaging Repository (TIR)
--

Defense Health Information Management System (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
- 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.

10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR 199.17, TRICARE Program; 45 CFR Parts 160 and 164, Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules; 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.

Background: Tele-radiology is the electronic transmission of radiological images from one location to another for the purposes of interpretation and / or consultation. Tele-radiology allows for timely interpretation of radiological images, greater access to secondary consultations (i.e., users in different locations may simultaneously view images), and greater continuing education than non-electronically transmitted radiology. Appropriately utilized, tele-radiology can improve access to quality radiological interpretations and thus significantly improve patient care.

Purpose: The Deployed Tele-Radiology System (DTRS), a Commercial Off The Shelf (COTS) product from MedWeb®, serves as the local Picture Archiving Communications System (PACS) providing tele-radiology services to deployed forces in Theater.

DTRS servers combine the functions of a PACS archive, Digital Imaging Communication in Medicine (DICOM) web server, telemedicine web server, Ethernet Proxy gateway, Virtual Private Network (VPN) encryption router, and satellite enhanced DICOM internet tunnel. DTRS servers receive, store, and transmit medical images acquired from diagnostic imaging devices (e.g., Computed Radiography (CR) x-ray, Computed Tomography (CT), and Ultrasound (US)). Diagnostic workstations running the Medweb client application provide for the presentation and manipulation of DTRS PACS images. DTRS also comes equipped with a barcode scanner that captures patient demographic information from a patient's Common Access Card (CAC) and transmits that information into DTRS. All of this diagnostic information is assembled on DTRS servers and is made available via a web interface in encrypted format over Wide Area Network (WAN) connections (i.e., satellite or written to self-playing CD-ROMs).

DTRS is also composed of laptop computers (Medweb Lites) that provide the same functionality as a full service DTRS. Medweb Lites are compact and portable. They are specifically targeted for use at smaller Level II Military Treatment Facilities (MTFs) in remote locations. These mobile systems are configured to be used at a particular site and are not removed from their protected work space without authorization.

The Theater Image Repository (TIR) is a new extended capability of DTRS. TIR will modify DTRS by adding a central, long term repository which will store all medical images collected and acquired by authorized users in Afghanistan, Iraq, and Kuwait. The goal of the TIR initiative will be to focus on the acquisition and storage of medical images that currently reside locally at the Level II and Level III MTFs. Medical images and artifacts from these facilities will be acquired and stored in the TIR. The TIR capability is comprised of diagnostic imaging devices which transmit digital images in standard DICOM format.

The types of personally identifiable information (PII) / protected health information (PHI) collected by DTRS / TIR includes:

- Name
- Social Security Number (SSN)
- Gender
- Birth date
- Medical information
- Military records

DTRS / TIR acquires, stores, and transmits PII / PHI from active duty military personnel deployed in Theater.

DTRS is owned by the Military Health System (MHS) / Department of Defense (DoD) and the systems are managed through a sustainment contract awarded by Defense Health Information Management System (DHIMS).

System Contact Information:

DHIMS
5109 Leesburg Pike
Skyline 6, Suite 100
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 associated with the collection of PII / PHI acquired, transmitted, and stored by DTRS / TIR are: 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 DTRS / TIR 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 user ID while logged on, and tracking user modification of data. System log files record system use and login attempts (successful and otherwise). DTRS / TIR information is reviewed by an authorized person to ensure accuracy, data security, and applicable Health Insurance Portability and Accountability Act (HIPAA) guidance. DTRS / TIR does not provide outgoing reports to other systems; the results of a diagnosis are entered manually into the Theater Medical Information Program (TMIP) Composite Health Care System (CHCS) Cache (TC2).

No classified data is processed by DTRS, and no classified data is communicated across the network. The information on DTRS / TIR 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, "Department of Defense Privacy Program." DTRS / TIR will support and comply with the appropriate DoD security requirements for encryption and compression of medical images and allow for storage expansion to accommodate a very significant increase of radiological images generated in Theater.

For the purposes of patient privacy, all data flowing outside the MTF, not specifically on a closed network, must be encrypted. DTRS / TIR allows for the acquisition of digital imaging studies, the storage of those studies, as well as the electronic transmission of studies to support clinical interpretation. Routing of images throughout an MTF's Local Area Network (LAN) is accomplished via Secure Socket Layer (SSL) encryption standard communication protocol known the Transmission Control Protocol / Internet Protocol (TCP / IP). MTF-to-MTF communication is accomplished via TCP / IP utilizing the DoD VPN.

The use of the Unclassified but Sensitive Internet Protocol (IP) Router Network (NIPRNET) or DoD VPN between all MTFs will comply with DoD, Service, and HIPAA policies. User IDs and passwords are required and password files are stored as encrypted files. CAC authentication may be required as well. System directories and files have read, write, and execute privileges set for selected functionality access rights by specific users. All DTRS / TIR users have formal access approval, a valid agency check at the appropriate level for information required to complete their job, and have signed nondisclosure agreements.

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.

TC2

Healthcare Artifact and Imaging Management Solution (HAIMS) – future upgrade

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 BaseTechnologies 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 (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."

MTF personnel with the appropriate level of certification will be granted access as a result of a National Agency Check with Written Inquires (NACI) or DoD-determined equivalent investigation and personnel on a need-to-know basis.

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.

Submission of PII is voluntary; however, if an individual refuses to provide information, comprehensive healthcare may not be possible.

If an individual wants to object to their PII being collected, they may do so by signing DD form 2871, "Request to Restrict Medical or Dental Information."

(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.

Consent to the specific uses of PII is obtained as necessary in accordance with DoD 5400.11-R, "Department of Defense Privacy Program," C.4.1.3.

PHI is collected for permitted uses and disclosures as set forth in DoD 6025.18-R, "DoD Health Information Privacy Regulation." Individuals are informed of these uses and are given the opportunity to authorize or restrict the use of their PHI based on the procedures in place at the local facility where the data is collected and maintained, in accordance with DoD 6025.18-R.

(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.	<p>This statement serves to inform you of the purpose for collecting personally identifiable information required by the Deployed Tele-Radiology System (DTRS) / Theater Imaging Repository (TIR) and how it will be used.</p> <p>AUTHORITY: 10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR 199.17 TRICARE Program; 45 CFR Parts 160 and 164, Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules; and E.O. 9397 (SSN), as amended.</p> <p>PURPOSE: To obtain from an individual the personally identifiable information necessary to appropriately identify and connect the individual's radiological images acquired, stored, or transmitted by the DTRS / TIR with that individual.</p> <p>ROUTINE USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records may specifically be disclosed outside the Department of Defense as a routine use pursuant to 5 U.S.C. 552(b)(3) as follows: to the Departments of Health and Human Services, Homeland Security, and Veterans Affairs, and to other federal, state, local, or foreign government agencies, and to private entities, including entities under</p>
----------------------------------	--

contract with the Department of Defense and individual providers of care, on matters relating to treatment of the individual, eligibility, claims pricing and payment, fraud, program abuse, utilization review, quality assurance, peer review, program integrity, third-party liability, coordination of benefits, and civil or criminal litigation.

DISCLOSURE: Voluntary: If an individual refuses to provide information, comprehensive healthcare may not be possible.

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.