



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Tele-Radiology System (MEDWEB)

Department of the Navy - TMA DHP Funded System - BUMED

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 IATS ID: 21738
- 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 N06150-2

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.

SORN authorities:

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 5131 (as amended), Bureau: names; location
10 U.S.C. 5132, Bureau: distribution of business; orders; records; expenses
44 U.S.C. 3101, Records Management by Agency Heads
10 CFR part 20, Standards for Protection Against Radiation
E.O. 9397 (SSN), as amended.

Other authorities:

10 U.S.C. 1095, Health Care Services Incurred on Behalf of Covered Beneficiaries: Collection from Third Party Payers Act
Medical and dental care in the DoD are authorized by Chapter 55 of Title 10 U.S.C., section 1071 - 1106
42 CFR 290DD Drug and Alcohol Treatment Records
5 CFR 293.502, Subpart E, Employee Medical File System Records
29 CFR Part 5, Labor Standards
5 CFR 339.101-306, Coverage
DoDD 6485.1 Human Immunodeficiency Virus-1 (HIV-1)
DoD Health Information Privacy Regulation

[Empty box]

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 Navy Tele-Radiology system (MEDWEB), offers integrated Current Procedure Terminology 4 (CPT4) templating, voice recognition dictation software, and the ability to distribute preliminary and final reports electronically to referring physicians. MEDWEB will be collecting medical information on patients which will include International Classification of Diseases 9 (ICD9) and Current Procedural Terminology (CPT) codes. The MEDWEB solution includes all hardware, software, and procedures required for secure, scalable, reliable, efficient, and interoperable medical image transmission and storage capabilities within Department of Defense (DoD) to include tactically deployed users. It provides the capability for the electronic transmission of radiological images and associated patient information and exams over a variety of telecommunication media to support clinical interpretation. It is used to transmit images from the remote site where the images are acquired to a Military Treatment Facility (MTF) for interpretation and consultation.

PII collected about an individual includes the Social Security Number, name, gender, birth date, and Medical information: Patient ID number, referring physician, modality type, institution name, exam date, exam type, study comments, patient history, findings, conclusion, provider name.

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

All systems are vulnerable to "insider threats." Radiology managers are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. There are defined criteria to identify who should have access to MEDWEB. These individuals have gone through extensive background and employment investigations.

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.

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.

Agilex, Inc.
The contract with Agilex 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 Law and Credit (NACLC).

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.

In the case of military personnel, the requested information is mandatory because of the need to document all active duty medical incidents in view of future rights and benefits. In the case of all other personnel/beneficiaries, the requested information is voluntary. If the requested information is not furnished, comprehensive health care may not be possible, but care will not be denied.

(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.

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

Describe each applicable format.

DD Form 2005 - Privacy Act Statement - Health Care Records provides:

Principal Purposes for which information is intended to be used:
This form provides you the advice required by The Privacy Act of 1974. The personal information will facilitate and document your health care. The Social Security Number (SSN) of member or sponsor is required to identify and retrieve health care records.

Routine Uses: The primary use of this information is to provide, plan and coordinate health care. As prior to enactment of the Privacy Act, other possible uses are to: Aid in preventive health and communicable disease control programs and report medical conditions required by law to federal, state and local agencies; compile statistical data; conduct research; teach; determine suitability of persons for service or assignments; adjudicate claims and determine benefits; other lawful purposes, including law enforcement and litigation; conduct authorized investigations; evaluate care rendered; determine professional certification and hospital accreditation; provide physical qualifications of patients to agencies of federal, state, or local government upon request in the pursuit of their official duties.

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.

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 Deployed Tele-Radiology System (DTRS)/Theater Imaging Repository (TIR) with that individual.

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

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.