



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Dental Digital Imaging (DDI) System

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
- 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.

SORN Authorities:

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 1095, Collection from Third Party Payers Act
10 U.S.C. 5131, as amended, Bureaus: names; location
10 U.S.C. 5132, Bureaus: distribution of business; orders; records; expenses
44 U.S.C. 3101, Records management by agency heads; general duties
10 CFR part 20, Standards for Protection Against Radiation
E.O. 9397 (SSN) as amended

Other authorities:

Medical and dental care in the DoD are authorized by Chapter 55 of Title 10 U.S.C., section 1071 - 1106

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.

Dental Digital Imaging (DDI) is a commercial off the shelf medical application that collects digital dental radiological images (x-rays) for the purpose of display and storage. The system is a diagnostic tool for Dentist examination of dental images. DDI collects radiological images from various dental modalities such as x-ray, computed axial tomography systems, and patient demographic information is scanned in from the front barcode of the member's Common Access Card (CAC) or the Dental Staff Member types it into DDI from the patient's paper-based dental record. DDI allows dental images to be easily shared across the health care enterprise by storing digital images in a central archive.

Navy Medicine currently uses Apteryx's DICOM Capture View (DCV) application and the data collected is detailed in this PIA.

Personally Identifiable Information (PII) collected about individuals includes: patient name, Social Security Number or the DoD ID number, gender, birth date, medical information to include the type of exam, and digital dental radiological images.

(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". The system administrator is vigilant to this threat by limiting system access to those individuals who have a defined, clinical need to access the information.

There are defined criteria to identify who should have access to the system. These individuals have gone through extensive background and employment investigations. The biggest privacy risk is user misuse of the system, e. g. not logging off, not "stripping" the PII from images stored in training files, etc. This risk is mitigated by mandating periodic training for all users.

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.

Diagnostic images are shared throughout the Navy healthcare enterprise for the purpose of diagnosing and treating patients.

Other DoD Components.

Specify.

Diagnostic Images are shared with Army and Air Force Medical and Dental Treatment Facilities worldwide.

Other Federal Agencies.

Specify.

Diagnostic images are transferred to the VA health system upon a member's separation from Active Duty.

State and Local Agencies.

Specify.

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

Specify.

Contractor: Apteryx. In accordance with DoD 6025.18-R "Department of Defense Health Information Privacy Regulation" the Contractor (Apteryx) meets the definition of Business Associate. 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 DoD 6025.18-R and DoD 8580.02-R, as amended. Additional requirements will be addressed when implemented.

(a) Definitions. As used in this clause generally refer to the Code of Federal Regulations (CFR) definition unless a more specific provision exists in DODI 6025.18-R. Individual has the same meaning as the term "individual" in 45 CFR 164.501 and 164.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g). Privacy Rule means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E. Protected Health Information has the same meaning as the term "protected health information" in 45 CFR 164.501, limited to the information created or received by The Contractor from or on behalf of The Government.

Electronic Protected Health Information has the same meaning as the term "electronic protected health information" in 45 CFR 160.103. Required by Law has the same meaning as the term "required by law" in 45 CFR 164.501 and 164.103.

Secretary means the Secretary of the Department of Health and Human Services or his/her designee.

Security Rule means the Health Insurance Reform: Security Standards at 45 CFR part 160, 162 and part 164, subpart C.

Terms used, but not otherwise defined, in this Clause shall have the same meaning as those terms in 45 CFR 160.103, 164.501 and 164.304.

(b) The Contractor shall not use or further disclose Protected Health Information other than as permitted or required by the Contract or as Required by Law.

(c) The Contractor shall use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Contract.

(d) The Contractor shall 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.

(e) The Contractor shall mitigate, to the extent practicable, any harmful effect that is known to the Contractor of a use or disclosure of Protected Health Information by the Contractor in violation of the requirements of this Contract.

(f) The Contractor shall report to the Government any security incident involving protected health information of which it becomes aware.

(g) The Contractor shall report to the Government any use or disclosure of the Protected Health Information not provided for by this Contract of which the Contractor becomes aware of.

(h) The Contractor shall ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by the Contractor on behalf of the Government agrees to the same restrictions and conditions that apply through this Contract to the Contractor with respect to such information.

(i) The Contractor shall ensure that any agent, including a subcontractor, to whom it provides electronic Protected Health Information, agrees to implement reasonable and appropriate safeguards to protect it.

(j) The Contractor shall provide access, at the request of the Government, and in the time and manner designated by the Government to Protected Health Information in a Designated Record Set, to the Government or, as directed by the Government, to an Individual in order to meet the requirements under 45 CFR 164.524.

(k) The Contractor shall make any amendment(s) to Protected Health Information in a Designated Record Set that the Government directs or agrees to pursuant to 45 CFR

164.526 at the request of the Government or an Individual, and in the time and manner designated by the Government.

(l) The Contractor shall make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by the Contractor on behalf of, the Government, available to the Government, or at the request of the Government to the Secretary, in a time and manner designated by the Government or the Secretary, for purposes of the Secretary determining the Government's compliance with the Privacy Rule.

(m) The Contractor shall document such disclosures of Protected Health Information and information related to such disclosures as would be required for the Government to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

(n) The Contractor shall provide to the Government or an Individual, in time and manner designated by the Government, information collected in accordance with this Clause of the Contract, to permit the Government to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528. **General Use and Disclosure Provisions**
Except as otherwise limited in this Clause, the Contractor may use or disclose Protected Health Information on behalf of, or to provide services to, the Government for treatment, payment, or healthcare operations purposes, in accordance with the specific use and disclosure provisions below, if such use or disclosure of Protected Health Information would not violate the Privacy Rule, the Security Rule, DoD 6025.18-R or DoD 8580.02-R if done by the Government. **Specific Use and Disclosure Provisions**

(a) Except as otherwise limited in this Clause, the Contractor may use Protected Health Information for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor.

(b) Except as otherwise limited in this Clause, the Contractor may disclose Protected Health Information for the proper management and administration of the Contractor, provided that disclosures are required by law, or the Contractor obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Contractor of any instances of which it is aware in which the confidentiality of the information has been breached.

(c) Except as otherwise limited in this Clause, the Contractor may use Protected Health Information to provide Data Aggregation services to the Government as permitted by 45 CFR 164.504(e)(2)(i)(B).

(d) Contractor may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1).

Obligations of the Government

Provisions for the Government to Inform the Contractor of Privacy Practices and Restrictions

(a) Upon request the Government shall provide the Contractor with the notice of privacy practices that the Government produces in accordance with 45 CFR 164.520, as well as any changes to such notice.

(b) The Government shall provide the Contractor with any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, if such changes affect the Contractor's permitted or required uses and disclosures.

(c) The Government shall notify the Contractor of any restriction to the use or disclosure of Protected Health Information that the Government has agreed to in accordance with 45 CFR 164.522. **Permissible Requests by the Government**

The Government shall not request the Contractor to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by the Government, except for providing Data Aggregation services to the Government and for management and administrative activities of the Contractor as otherwise permitted by this clause.

Termination

(a) Termination. A breach by the Contractor of this clause, may subject the Contractor to termination under any applicable default or termination provision of this Contract.

(b) Effect of Termination.

(1) If this contract has records management requirements, the records subject to the Clause should be handled in accordance with the records management requirements. If this contract does not have records management requirements, the records should be handled in accordance with paragraphs (2) and (3) below

(2) If this contract does not have records management requirements, except as provided in paragraph (3) of this section, upon termination of this Contract, for any reason, the Contractor shall return or destroy all Protected Health Information received from the Government, or created or received by the Contractor on behalf of the Government. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of the Contractor. The Contractor shall retain no copies of the Protected Health Information.

(3) If this contract does not have records management provisions and the Contractor determines that returning or destroying the Protected Health Information is infeasible, the Contractor shall provide to the Government notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Government and the Contractor that return or destruction of Protected Health Information is infeasible, the Contractor shall extend the protections of this Contract to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as the Contractor maintains such Protected Health Information.

Miscellaneous

(a) Regulatory References. A reference in this Clause to a section in DoD 6025.18-R, DoD 8580.02-R, Privacy Rule or Security Rule means the section as in effect or as amended, and for which compliance is required.

(b) Survival. The respective rights and obligations of Business Associate under the "Effect of Termination" provision of this Clause shall survive the termination of this Contract.

(c) Interpretation. Any ambiguity in this Clause shall be resolved in favor of a meaning that permits the Government to comply with DoD 6025.18-R, DoD 8580.02-R, Privacy Rule or Security Rule

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.

Individuals may decline to provide their PII; however, failure to do so may result in limited or no services being provided.

The information is used for dental and medical treatment purposes. The PII is used to associate the images to the proper patient.

(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.

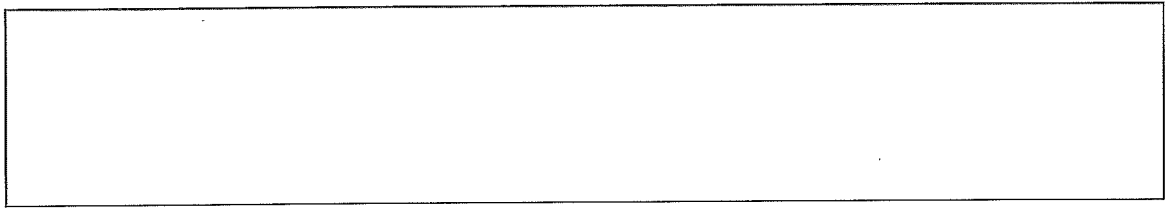
(2) If "No," state the reason why individuals cannot give or withhold their consent.

The information is used for dental and medical treatment purposes.

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>DD Form 2005 - Privacy Act Statement - Health Care Records provides:</p> <p>Principal Purposes for which information is intended to be used:</p> <p>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.</p> <p>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.</p>
----------------------------------	---



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.