



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Digital Dental X-Ray System (DDX)

Department of Navy - USMC

### **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 N06150-2 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.

The Digital Dental X-Ray (DDX) system is a commercial off-the-shelf medical system used to generate and review dental imagery. Dental imagery is not maintained or stored on the system, but is removed from the system and either sent with the patient on DVD/CD-ROM, or transferred to an authorized HIPPA-compliant computer system. Backups of data and imagery is backed up to external USB Solid State Drives (SSDs) in accordance with unit policy.

The DDX system utilizes Apteryx's X-Ray Vision® DICOM Capture View (DCV) application.

Personally Identifiable Information (PII) collected about individuals includes: patient name, 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.

DDX system is vulnerable to insider threats. System is standalone and not vulnerable to remote attacks. System administrators are responsible for applying updates released by program office and support activities. Access to DDX system is controlled by system owner based on need-to-know. The system administrators provide unique user accounts requiring username and password for logon. Windows 7 BitLocker encryption is used to safe guard against unauthorized disclosure of patient health information (PHI). Additionally, the DDX system itself is stored in an access-controlled USMC medical facility. Accounts on the DDX system are controlled per-user and imagery stored by a user is not by default provided to other users. No group accounts are permitted on the DDX system.

There are defined criteria to identify who should have access to the system. These individuals have gone through extensive background and employment investigations. User access must be authorized by the unit senior dental officer. 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 annual training for all users and periodic audits by the system administrator.

**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.

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 to the dental officer at time of treatment; however, failure to do so may result in limited or no services being provided. The information is used for dental and medical treatment purposes.

(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.

Medical and dental staff requires the PII in order to associate the images to the proper patient and to update the patient's dental record.

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.  
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.

**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.**