PRIVACY IMPACT ASSESSMENT (PIA)

For the

Dental Common Access System (DENCAS)

Defense Health Agency (DHA)

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

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, Health Care Services Incurred on Behalf of Covered Beneficiaries: Collection from Third Party Payers Act
10 U.S.C. 5132, Bureaus: distribution of business; orders; records; expenses
44 USC 3101, Records management by agency heads; general duties
10 CFR Part 20, Standards for Protection Against Radiation
EO 9397 (SSN), as amended.
(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.

DENCAS is a web based application that is used to collect, collate, warehouse, and report on dental recall, readiness, and productivity.

At the corporate level, the Director of Navy Dentistry can view patient and productivity data either Navy-wide or drill down to various Navy Dental Commands. Dental liaisons at bases and in the fleet are able to view their Unit’s dental readiness and obtain a list of individuals who need to be sent for dental treatment or for exams.

Two types of data are kept – patient treatment data and provider data (number of procedures, patients, etc.) which is historical for metrics. The provider data can show number of treatments at all levels but is not patient specific.

The only patient specific data stored is on present health status and dental needs. There is no historical treatment data retained.

The types of personal information about individuals collected in the system include name, social security number (SSN), DoD Electronic Data Interchange Personal Identifier (EDIP/I)/other ID number, date of birth, dental treatment information, personal telephone number, home address, and work/personal e-mail addresses. SSN still required at this time to support Navy Readiness systems that receive dental readiness data. Personnel information is maintained on active duty personnel and only dependents who are stationed overseas with their sponsors.

DENCAS is managed by DHA/J-6 Health Information Technology/Solutions Delivery Division/PM Clinical Support.

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

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that DENCAS, with its collection of PII, could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place.

DENCAS is hosted at the Space and Naval Warfare Systems Center (SPAWAR) New Orleans, Louisiana (NOLA). The data center provides physical security and prevents unauthorized personnel from gaining access to equipment, facilities, materials and documents by use of door badge readers. Assets are safeguarded against espionage, sabotage, damage, fire and theft by electronic means with the use of a security system, fire alarms and sprinkler equipment. Access to NOLA is restricted to authorized personnel only.

DENCAS data is encrypted in transit.

DENCAS has a disaster recovery site, which is a mirror image of the production site. The data is backed up to the disaster recovery site on a daily basis.

Data is reviewed by users on a regular basis to ensure data integrity, availability, accuracy, and relevancy. Any issues are brought to the attention of the DENCAS support team to correct.

Users are required to take annual HIPAA/PII training.
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. Army and Air Force; This information can be shared with all Navy and Marine Corps dentists to determine dental readiness of all Navy and Marine Corps dental patients.

☐ Other Federal Agencies.

Specify.

☐ State and Local Agencies.

Specify.

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

Specify. The vendor, GRSi, provides programming, development, and Help Desk support for the DENCAS product. In almost all cases where the vendor handles trouble tickets and modifications to a system that contains PII they will have access to PII through the system.

The contract support agreements include the standard Military Health System (MHS) HIPAA Business Associate Agreement, thereby requiring compliance with DoD information security and privacy policies for PII and PHI. The contract also requires compliance with all applicable privacy and security laws and regulations, including data breach reporting and response requirements, in accordance with DFAR Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoDD 5400.11, DoD Privacy Program, and DoD 5400.11-R, Department of Defense Privacy Program. The contractor must also comply with the Freedom of Information Act (DFAR Subpart 224.2).

☐ 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.

The information is used for dental readiness purposes only. It is a requirement that a service member's dental readiness status be provided to proper authorities as it impacts their ability to deploy overseas. For other information collected DENCAS is not the initial point of collection.

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 readiness purposes only. It is a requirement that a service member's dental readiness status be provided to proper authorities as it impacts their ability to deploy overseas. For other information collected DENCAS is not the initial point of collection.

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.

Prior to receiving a dental exam, the patient is required to provide the clinic with a signed Privacy Act Statement form. That form covers all dental activities to include DENCAS.

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

PRIVACY ACT STATEMENT - HEALTH CARE RECORDS
This form is not an authorization or consent to use or disclose your health information.
1. AUTHORITY FOR COLLECTION OF INFORMATION INCLUDING SOCIAL SECURITY NUMBER
10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. Chapter 55, Medical and Dental Care; 42 U.S.C. Chapter 32, Third Party Liability for Hospital and Medical Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); DoDI 6055.05, Occupational and Environmental Health (OEH); and E.O. 9397 (SSN), as amended.

2. PRINCIPAL PURPOSES FOR WHICH INFORMATION IS INTENDED TO BE USED:

Information may be collected from you to provide and document your medical care; determine your eligibility for benefits and entitlements; adjudicate claims; determine whether a third party is responsible for the cost of Military Health System (MHS) provided healthcare and recover that cost; evaluate your fitness for duty and medical concerns which may have resulted from an occupational or environmental hazard; evaluate the MHS and its programs; and perform administrative tasks related to MHS operations and personnel readiness.

3. ROUTINE USES:

Information in your records may be disclosed to: Private physicians and Federal agencies, including the Department of Veterans Affairs, Health and Human Services, and Homeland Security (with regard to members of the Coast Guard), in connection with your medical care; Government agencies to determine your eligibility for benefits and entitlements; Government and nongovernment third parties to recover the cost of MHS provided care; Public health authorities to document and review occupational and environmental exposure data; and Government and nongovernment organizations to perform DoD-approved research.

Information in your records may be used for other lawful reasons which may include teaching, compiling statistical data, and evaluating the care rendered. Use and disclosure of your records outside of DoD may also occur in accordance with 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, which incorporates the DoD Blanket Routine Uses published at: http://dpcld.defense.gov/privacy/SORNsIndex/BlanketRoutineUses.aspx.

Any protected health information (PHI) in your records may be used and disclosed generally as permitted by the HIPAA Privacy Rule (45 CFR Parts 160 and 164), as implemented within DoD by DoD 6025.18-R. Permitted uses and disclosures of PHI include, but are not limited to, treatment, payment, and healthcare operations.

4. WHETHER DISCLOSURE IS MANDATORY OR VOLUNTARY AND EFFECT ON INDIVIDUAL OF NOT PROVIDING INFORMATION:

Voluntary. If you choose not to provide the requested information, comprehensive health care services may not be possible, you may experience administrative delays, and you may be rejected for service or an assignment. However, care will not be denied.

This all inclusive Privacy Act Statement will apply to all requests for personal information made by MHS health care treatment personnel or for medical/dental treatment purposes and is intended to become a permanent part of your health care record.

Your signature merely acknowledges that you have been advised of the foregoing. If requested, a copy of this form will be furnished to you.