PRIVACY IMPACT ASSESSMENT (PIA)

For the

Dental Common Access System (DENCAS)
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**	☐	**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	54
☐	**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 007-000000074

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 USC 1095, collection from Third Party Payers Act
10 USC 5131, as amended, and 5132, BUREAUS; OFFICE OF THE JUDGE ADVOCATE GENERAL
44 USC 3101, Records management by agency heads; general duties
10 CFR Part 20, Standards for Protection Against Radiation
EO 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.

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), date of birth, dental treatment information, and work e-mail addresses.

(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.

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. This information can be shared with all Navy and Marine Corps dentists to diagnose and treat all Navy and Marine Corps dental patients.

☒ **Other DoD Components.**

Specify. Army, Air Force, Coast Guard (Public Health)

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify.

ASMR - Vendor 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.

Para 4.3.2. Protection of Patient Information
The Contractor shall maintain, transmit, retain in strictest confidence, and prevent the unauthorized duplication, use, and disclosure of patient information in accordance with Standards for Privacy of Individually Identifiable Health Information, Final Rule, December 28, 2000 (effective April 14, 2001) and The Privacy Act of 1974. The Contractor shall provide patient information only to employees, contractors, subcontractors, and Government personnel having a need to know such information in the performance of their duties for this project.

Para 4.3.3. Compliance with DoD Privacy Regulations
The Contractor shall comply with the most current version, and all future changes when released, of all Government and DoD privacy regulations and directives and other applicable Service privacy instructions and regulations. In addition, the Contractor shall comply with the most current version and all future changes when changes are released, of all relevant rules published in the Federal Registrar to implement the HIPAA of 1996. This shall include Standards for Privacy of Individually Identifiable Health Information, Final Rule, published December 28, 2000.

☐ **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.

(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.

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:
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.

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.