PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Naval Health Clinic Cherry Point (NHCCP)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

03/10/2026

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- ☐ From members of the general public
- ☐ From Federal employees
- ☒ from both members of the general public and Federal employees
- ☐ Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

- ☐ New DoD Information System
- ☐ New Electronic Collection
- ☒ Existing DoD Information System
- ☐ Existing Electronic Collection
- ☐ Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The NHCCP Enclave Area of Responsibility (AOR) stretches across Marine Corps Air Station Cherry Point in Eastern North Carolina, consisting of 1 Health Care facility that provide patient care. The NHCCP Enclave is a conglomeration of IM/IT systems servicing Naval Health Clinic Cherry Point, as well as Occupational Health, IOP, ASTC and Army Vet Clinic. The facility is located on a military gated and guarded installation with controlled power and environment conditions.

NHCCP provides out-patient care to Active Duty, Reservists, select DoD Civilian employees, retirees and their dependents. Personal information collected is limited to those pieces of information necessary to maintain employee records, establish accounts and provide enhanced patient reporting for NHCCP staff clinicians. The current Electronic Health Record (EHR) consists of MHS GENESIS Patient Portal and Essentris. All PII/PHI collected is used solely for identification and authentication for the purpose of administrative and/or patient care and services.

The NHCCP Enclave is on the legacy NMED network and in the process of migrating all systems to MEDCOI_Cherry Point. NHCCP systems consist of clinical and administrative servers, Application and Web Servers and associated network components. NHCCP utilizes only DHA approved applications and services. All servers and computers are compliant with current Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) requirements. Network traffic is internal to the enclave and encrypted. NHCCP maintains a local Microsoft SQL 2008 Enterprise database server and is currently in the process of migrating to a local Microsoft SQL 2014 database server.

The following PII information is collected to support command operations:

- Full names of staff and select beneficiaries
- Date of Birth
- DOD EDIPI Numbers
- Security Clearance Status
- Telephone Numbers (Home and cell)

Home and cell phone numbers

Financial and medical information is collected and processed only by other DHA approved programs and systems in use within the enclave.

NHCCP also maintains an "Operational Database System (ODS)" which allows system administrators the ability to query patient information from multiple Medical Program of Record platforms (ie. AHLTA, CHCS and ESSENTRIS) in order to be data warehoused to provide support to the Health Clinic beyond the capabilities presently offered within the varied program of record systems utilized at NHCCP. These systems include Surgery Scheduling System (S3), Lab Dashboard, Right Fax, IMED Consent, MRS, and Johnson Controls badging & video systems. as well as several in-house custom applications such as , Transfer Center and Provider Deductions.

PII collected by NHCCP is used solely to link the various clinical data systems or to complete required information in official forms and reporting.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

The PII collected by systems, applications, and electronic collections utilizing the LAN is generally intended for administrative and mission-related use.

e. Do individuals have the opportunity to object to the collection of their PII? ☒ Yes ☐ No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

NHCCP personnel voluntarily offer their information. However, withholding of information will impact their ability to participate and gain access to the Naval Health Clinic Cherry Point Enclave and supported clinical applications.

f. 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.

NHCCP personnel voluntarily offer their information. However, withholding of information will impact their ability to participate and gain access to the Naval Medical Center Camp Lejeune Enclave and supported clinical applications.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☒ Privacy Act Statement ☒ Privacy Advisory ☐ Not Applicable

The Privacy Act of 1974 imposes responsibilities to prevent misuse or compromise of data, or information, contained in DoD information systems. It contains three main provisions.
a. Confidentiality of Information - A large amount of information in our information systems is sensitive, personal, medical information. Only authorized people or agents are allowed to disclose this information. Additional federal law imposes penalties for illegally using this type of information. Personal data may not be accessed unless necessary for an official purpose.
b. Data Integrity- Patient treatment decisions are made from information stored on Naval Medical Center Camp Lejeune information systems. Users inputting data into computer systems are required to ensure the information is accurate, timely, and relevant.
c. Data Security - The third provision of the Privacy Act requires in place safeguards to ensure confidential and correct records. This entails protective measures, such as ID/Passwords and access/verify codes, to protect data that might otherwise be corrupted and thus affect correct medical care.
You are responsible for following all security-related guidelines as set forth in Navy and local directives. Your ID/Password and/or access/verify codes are unique to you. These codes must be kept confidential.
Your identification codes are necessary for you to perform your job duties. Memorize your codes. If you feel any of your codes have been compromised, immediately change your code(s) or notify the MID trouble desk for help. Remember, the ID/Password or access/verify code represents a handwritten signature and are legally equal to a handwritten signature.
It is important you recognize the fact that NHCCP Information Systems are Federal Interest Automated Information Systems protected by various federal laws. They may be accessed and used by authorized personnel only. All activities of personnel using these systems may be monitored. This includes keystroke capture and analysis. Anyone using this system expressly consents to such monitoring and is advised that any evidence of unauthorized or criminal activity will be provided to the appropriate authorities.
l have read and understand the security guidelines above as well as the contents of OPNAV 5239/(14), which prohibits misuse of systems or the information contained in the system under penalty of disciplinary action. I understand the necessity for safeguarding my USER ID/Password, and recognize the requirement for maintaining the confidentiality and integrity of the information contained in NHCCP Information systems. I further understand if l divulge information under the Health Insurance Portability Accountability Act of l 996 and Privacy Act of 1974, I may be prosecuted under the Uniform Code of Military Justice, rules governing the conduct of civilian personnel, or, in the case of contract workers, be referred to NHCCP Contracting Services for appropriate actions.
This is a legally binding document. Ensure you understand it before you apply your signature.

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	NHCCP Healthcare Provider, Human Resources, IS Administrators, MTF Personnel (USERS)
☐ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	
☐ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	

☐ State and Local Agencies — Specify.

☐ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)* — Specify.

☐ Other *(e.g., commercial providers, colleges)*. — Specify.

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☒ Individuals
☒ Existing DoD Information Systems
☐ Other Federal Information Systems
☐ Databases
☐ Commercial Systems

Mammography Reporting Systems (MRS)
Defense Medical Human Resource System internet (DHMRSi)
Tricare Online (TOL)
Health Artifact and Image Management Solution (HAIMS)
Centralized Credentials Quality Assurance System (CCQAS)
DHA Global Service Center
IMED Consent
Defense Information Security System (DISS)
MHS GENESIS Patient Portal
Synovium 360
Joint Legacy Viewer
Armed Forces Billing and Collection Utilization Solution (ABACUS)

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

☐ E-mail
☐ In-Person Contact
☐ Fax
☒ Information Sharing - System to System
☐ Other *(If Other, enter the information in the box below)*
☒ Official Form (*Enter Form Number(s) in the box below)*
☒ Paper
☐ Telephone Interview
☒ Website/E-Form

Refer to the PIA specific to the system, application, or electronic collection hosted on the LAN for additional information.

k. 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 must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier EDHA07

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date.

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. Not Applicable

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

The LAN/Enclave/Hosting platform itself does not have a NARA approved, pending, or GRS authority and retention instructions applied as a whole. Refer to NARA approved, pending, or GRS authority and retention instruction specific to the systems, applications, electronic collections, file servers, and share drives contained within the LAN/Enclave

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

5 U.S.C. 301, Department Regulation;
10 U.S.C., Chapter 55; Pub.L. 104-91, Health Insurance Portability and Accountability Act of 1996;
DoD 6025.18-R, DoD Health Information Privacy Regulation;
10 U.S.C. 1071-1085, Medical and Dental Care;
42 U.S.C. Chapter 117, Sections 11131-11152, Reporting of Information;
10 U.S.C. 1097a and 1097b, TRICARE Prime and TRICARE Program;
10 U.S.C. 1079, Contracts for Medical Care for Spouses and Children;
10 U.S.C. 1079a, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS);
10 U.S.C. 1086, Contracts for Health Benefits for Certain Members, Former Members, and Their Dependents;
DoD Instruction 6015.23, Delivery of Healthcare at Military Treatment Facilities (MTFs);
DoD 6010.8-R, CHAMPUS;
10 U.S.C. 1095, Collection from Third Party Payers Act; and E.O. 9397 (SSN)
E.O. 9397 (SSN)

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

Per DoDM 8910.01 Vol 2 "Current federal employees are considered members of the public if the collection of information is addressed to them in their capacity as individual private citizens. Federal employees are not considered members of the public when they respond to a collection of information within the scope of their employment (includes all the tasks performed to accomplish the job they perform for the federal agency). The latter is considered a DoD internal information collection and must be approved and licensed in accordance with the procedures in DoDM 8910.01, Vol 1,
All information collection performed within the Naval Health Clinic Cherry Point Enclave is either "DoD Internal information collection" or inherited through System to System transfer as it is further housed internally. These are both covered under DHA System of Records Notice (SORN) already established.