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 Research Center (NHRC) MedCOI

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

04/05/24

Bureau of Medicine and Surgery (BUMED)

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
- [x] 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
- [x] 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 Naval Health Research Center (NHRC) MedCOI is comprised of the following: Hardware, Software, Security Appliances, Networking Devices, Telecommunications Architectures, Office Automation, Medical and Administrative Servers, File and Application Servers, and internal Web Servers. Commercial-Off-The-Shelf (COTS) applications such as Microsoft Word, Excel, PowerPoint, and Outlook are utilized to provide administrative support to the enclave and may process personally identifiable information (PII).

The enclave hosts multiple SQL databases and servers to support various research protocols to include the following but not limited to: Career History Archival Medical and Personnel System (CHAMPS), Millennium Cohort Study Program (MCS), Recruit Assessment Program (RAP), U.S. Marine Corps (USMC) Resilience Protocol, Expeditionary Medical Database (EMED), Valor Wounded Warrior Recovery Program and Birth and Infant Health Research (BIHR) Program.

Research data management involves collecting, maintaining, using and disclosing of personally identifiable information (PII) and protected health information (PHI) to researchers and other authorized personnel on the NHRC Network. The research data collected is from dependents, retirees, active duty, permanent resident aliens, former spouses, Reservists and National Guard members. Data is collected from the following categories of individuals - Military Personnel (Active Duty, Reserve, Retirees and Dependents) for Army, Navy, Air Force, Marines, Space Force, and National Guard. Personnel as applicable from Coast Guard, Public Health Services, Local Nationals, Federal Civilians (Department of Defense (DoD), Army, Navy, Air Force, Marines, Space Force and VA), Contractors, and Volunteer personnel. The data is obtained from existing DoD information systems and collections. The data collected is used to respond to inquiries from military leadership, military medical providers, DoD and DHA policy makers, and to conduct research with the ultimate aim of ensuring the welfare of military members and their families.

The information is being protected by storage in a discretionary file system (DFS) with data encryption where applicable.

PII may be disseminated/transferred in some systems, applications, and available within documents stored on file servers and shared drives. The administrative, physical, and technical security controls that protect the confidentiality of PII in these systems, applications, and electronic collections are addressed in separate privacy impact assessments (PIA). The PIAs are available at: https://dodcio.defense.gov/In-the-News/Privacy-Impact-Assessments/aspx/.

All Servers are compliant with the current Defense Information Systems Agency (DISA) Security Technical Implementation Guidelines (STIG) and Defense Health Agency (DHA) cybersecurity requirements.

The NHRC MedCOI Enclave is managed by the Command Information Officer, Information System Security Manager ((ISSM) and Information System Security Officer (ISSO). Each Program Manager or Researcher is responsible for managing the databases and data

assets containing PII within their respective areas of responsibility.

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 purpose and the intended use of the collected PII is specific to an information system and is addressed in the system's privacy impact assessment (PIA).

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.

The opportunity for individuals to object to the collection of PII is specific to the method used to collect PII in the respective information system and is addressed in the respective system's PIA.

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.

The opportunity for individuals to consent to uses of PII is specific to the method used by the respective information system and is addressed in the respective system's PIA.

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 MEDCOI infrastructure does not collect PII directly from individuals; however, system components, applications, and electronic collections within the enclave might collect PII. Refer to the respective system component, application, or electronic collection PIA for additional information.

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.	PII may be shared with personnel with authorized access to the MEDCOI.
☐ 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.	NHRC has numerous contractors such as GDIT and Leidos Inc. The language in the contracts include appropriate FAR privacy clauses 52.224-1, Privacy Act Notification and 52.224-2, Privacy Act. The contract Performance Work Statement (PWS) has Business Associate Agreement (BAA) language. As outlined in the contract, access to sensitive IT systems is contingent upon a favorably adjudicated background investigation. When access to IT systems is required for performance of the contractor employee's duties, such employees shall in-process with the Navy Command's Security Manager and Information Assurance Manager upon arrival to the Navy command and shall out-process prior to their departure at the completion of the individual's performance under the contract. Completion and approval of a System Authorization Access Request Navy (SAAR-N) form is required for all individuals accessing Navy Information Technology resources. The decision to authorize access to a government IT system/ network is inherently governmental. The contractor supervisor is not authorized to sign the SAAR-N; therefore, the government employee with knowledge of the system/ network access required or the COR shall sign the SAAR-N as the "supervisor". The Business Associate may only use or disclose PHI as necessary to perform the services set forth in the Agreement or as required by law. The Business Associate is not permitted to de-identify PHI under DoD HIPAA issuances or the corresponding 45 CFR 164.514(a)-(c), nor is it permitted to use or disclose de-identified PHI, except as provided by the Agreement or directed by the Covered Entity. The Business Associate agrees to use, disclose and request PHI only in accordance with the HIPAA Privacy Rule "minimum necessary" standard and corresponding DHA policies and procedures as stated in the DoD HIPAA Issuances.
☐ Other *(e.g., commercial providers, colleges)*.	Specify.	Not applicable for the enclave. PII sharing is addressed in the respective system's PIA.

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

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

Not applicable for the NHRC MedCOI; the source of the PII collected is specific to the information system component and is addressed in the sub-system's PIA.

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

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

Not applicable for the NHRC MedCOI; the information collection method is specific to the information system component and is addressed in the sub-system's PIA.

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 | Not Applicable.

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.

Not applicable for the NHRC MedCOI; MedCOI is not used to retrieve records by personal identifier, therefore a SORN is not necessary.

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. | GRS 3.2 Item 010; DAA-GRS-2013-0006-0001

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

(3) Retention Instructions.

Destroy audit logs 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system. 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.

Authorities to collect information are specific to the information system component and addressed in the respective sub-system's PIA.

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.

The NHRC MedCOI enclave does not collect information from members of the public; however, system components, applications, or electronic collections within the NHRC MedCOI enclave might do so. Refer to the specific sub-system, application, or electronic collection PIA for information regarding the OMB Control Number.