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:

Program Executive Office Defense Healthcare Management Systems System Development Life Cycle NEXT / PEO DHMS SDLC NEXT

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

06/05/2025

Defense Healthcare Management Systems System Development Life Cycle

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.

PEO DHMS SDLC NEXT provides a standardized environment, services, and resources to facilitate the effective development and testing of healthcare management systems, applications, and their capabilities.

The PII/PHI collected within the system is a combination of PII used to authenticate users into the system environment (CAC data), and PHI which includes de-identified clinical data.

All test data managed and maintained to support development within the PEO DHMS SDLC is de-identified patient data, categorized as PII/ PHI according to best practices. The PEO DHMS SDLC is not interconnected to MEDCOI or any production healthcare systems. Only U.S. Federal contractors with a valid Common Access Card (CAC) have access to the system.

The system is owned and managed by Program Executive Office - Defense Health Management System (PEO - DHMS).

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 is required to implement and operate identification and authorization processes for PEO DHMS SDLC NEXT information technology. For Authentication, The CAC data is only used to validate that the user has a current, non-revoked, unexpired, DoD-issued private key certificate and a current, matching user account with associated individual or group authorization rights on the system. The data is revalidated at each log-on to the system.

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.

PEO DHMS SDLC NEXT is not the initial point of collection of the PII/PHI, CAC data. If that data was not available for a specific individual, then that individual would not be able to access the PEO DHMS SDLC system, which is required for day-to-day operations. PHI information gathering will be maintained by a subset of PEO DHMS SDLC NEXT . Individual's PII, for system authentication purposes, cannot be removed without terminating system access for that individual, as no unauthenticated access is allowed. Individuals PHI can only be removed from the system by appointed personnel. The collected PII data is a subset of the data collected by the DoD Identity Synchronization Service (IdSS) and contained in the individuals CAC. Individuals seeking to determine whether information about themselves is contained in the IdSS can email the Defense Information Systems Agency (DISA) at disa.meade.esd.list.idam-eds@mail.mil or address written inquiries to DISA, Enterprise Services Directorate, P.O. Box 549, Fort George Meade, MD 20755-0549.

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 PII/PHI is required to implement and operate identification and authorization processes for PEO DHMS information technology. Users must identify themselves to take any action on the system, including any action to give or withhold consent. If that data were not available for a specific individual, because for example the individual does not consent to use of his/her CAC data, then that individual would not be able to access the PEO DHMS SDLC NEXT system, which is required for individuals to do their work.

PHI/PHI pertaining to specific individuals not required for system access IE Special Handling PII, is handled/maintained by official appointed personnel and cannot be shared with external entities outside of the specific individual on which the information describes.

PEO DHMS SDLC NEXT cannot remove the individual's PII needed for system access without terminating said system access for that individual, as no unauthenticated access is allowed. The collected data is a subset of the data collected by the IdSS and contained in an individual's CAC.

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

This system is not the initial collection point for the PII. The PII is obtained from an existing DoD information system or electronic collection, therefore no Privacy Act Statement or Privacy Advisory is required.

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.	
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	CAC data is validated electronically to DoD Online Certificate Status Protocol (OCSP) sites, which are maintained by DISA as part of the IdSS.
☐ 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.	Various contractors develop, operate and maintain the system for internal use. American Systems Corporation Deloitte All must maintain the appropriate background investigations based on their specific roles and responsibilities. The contract requires the developer, DNC, to "establish appropriate administrative, technical, and physical safeguards to protect any and all data, to ensure the confidentiality, integrity, and availability of said data. At a minimum, this shall include provisions for personnel security, electronic security and physical security."
☐ 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 ☒ Databases

☒ Existing DoD Information Systems ☐ Commercial Systems

☒ Other Federal Information Systems

Individuals provide the CAC, Personal Identity Verification (PIV), and Electronic Data Interchange Personal Identifier (EDIPI, n/k/a DoD ID) issued by Defense Manpower Data Center (DMDC) via RAPIDS / DEERS, as part of their individual CAC. PEO DHMS SDLC NEXT exchanges certificate information with the CAC electronically, and validates the certificate through the Online Certificate Status Protocol (OCSP) to DISA, which maintains certificate revocation listing sites. PEO DHMS SDLC NEXT does not exchange data directly with DMDC, RAPIDS, or DEERS.

Personnel PII not required for system access will be collected and maintained through a centralized database and will only be available at the request of those users.

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

Individuals fill out a PEO DHMS SDLC NEXT Access Request Form (PEO_FRM_RemoteAccessForm_v6.4._-March_26_2020-blank.pdf), which must be signed with their CAC.

PII not required for system access will be collected by the hiring agency for each specific personnel, as per their internal on-boarding process

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

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.

The only PII collected is related to user onboarding and account creation. No information, such as birth date, SSN, etc is collected. The DHA SORN is inherited by PEO DHMS SDLC Next.

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 3.1, item 011 (DAA-GRS- 2013-0005- 0007)

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

(3) Retention Instructions.

FILE NUMBER: 1601-01
FILE TITLE: System Development Records
DISPOSITION: Temporary. Cut off after system is superseded by a new iteration, or is terminated, defunded, or when no longer needed for administrative, legal, audit, or other operational purposes. Destroy 5 years after cutoff.

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, Departmental Regulation; 10 U.S.C. Chapter 8, Defense Agencies and Department of Defense Field Activities; DoD Directive

5105.19, Defense Information Systems Agency (DISA); DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Enterprise User Data Management Plan of Persons and Personas, August 11, 2010; Global Information Grid 2.0 Concept of Operations (GIG 2.0 CONOPS), March 11, 2009.

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.

PEO DHMS SDLC NEXT is not publicly accessible and does not collect information from members of the public. Only individually authorized military, federal employees, or sponsored federal contractors assigned to work for PEO DHMS may request and be granted access to the system.