

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:

Defense Healthcare Management System Modernization Electronic Health Record (DHMSM EHR)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

8/26/2022

Defense Healthcare Management System Modernization (DHMSM) PMO

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 Defense Healthcare Management System Modernization (DHMSM) Electronic Health Record (EHR) system is the core component of the Military Health System (MHS) GENESIS system. DHMSM EHR provides access to authoritative clinical data sources, and is the authoritative source of clinical data supporting improved population health, patient safety, and quality of care to maximize medical readiness for the Department of Defense (DoD). As the modernization effort continues, the DHMSM EHR system will gradually replace the legacy EHR systems and become MHS GENESIS. Hereinafter, DHMSM EHR is referred as MHS GENESIS.

MHS GENESIS is an EHR information system that collects, processes, and distributes EHR longitudinally across the Military Health System (MHS), Department of Veterans Affairs (VA), United States Coast Guard (USCG), TRICARE network of service providers, and other Federal agencies from approximately 9.6 million DoD active duty personnel and their dependents.

MHS Genesis currently consists of the following subsystems:

Infrastructure: Provides the core networking services and shared tools/services for MHS Genesis.

EHR Core: Provides the primary clinical suite of software for MHS Genesis.

High Assurance Clinical Application Services (HA-CAS): Provides additional solutions to the primary EHR Core suite of applications, ie Patient Portal, HealtheIntent, CAMM7, Dragon Nuance, Health Information Exchange (HIE), Cloud IAM and Millennium Cloud Services.

Test: Provides a testing environment for MHS Genesis.

Train: Provides a training environment for MHS Genesis users.

Build: Provides an environment for dedicated to wave deployment, specifically the enterprise build, localized build and testing. It is currently in use by Initial Operating Capacity developers and as well as local site experts engaged in deployment activities, including design and configuration Workshops (National and Local), System Validation Sessions and Integration Validation.

DHMSM System of Record: provides centralized management of MHS GENESIS policies and documentation.

Personally Identifiable Information (PII) collected, processed, and distributed includes demographic information, personal contact information, Social Security Numbers (SSNs), emergency contact information, employment information, disability information, child information, and religious preference, medical information, and Protected Health Information (PHI). These categories of PII are collected from DoD, VA, and USCG beneficiaries and their family members for the timely and high quality delivery of health care services and the determination and processing of patient benefit information for DoD, VA, USCG, and other beneficiaries, as well as for Defense Health Agency (DHA) authorized clinical trials, medical research, and disease registries.

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 collected for mission-related and administrative, for patient identification, verification, and authentication in the course of

scheduling and administering medical treatment; and for data matching when interfacing and sharing data with external medical and healthcare provider systems.

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 individual can object by not signing the forms DD Forms 2870 and 2871, or by filing a complaint with the local Military Treatment Facilities (MTFs) Privacy Office, or in writing with the DHA Privacy and Civil Liberties Office (PCLO).

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.

At the MTF, individuals consent to the specific uses of their PII by submitting DD Form 2870 and request restrictions on the use of the PHI by submitting DD Form 2871. Refusal to consent may affect the provisioning of care to the patient.

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

AUTHORITY: 10 USC 8111, Sharing of Department of VA and DoD Healthcare Resources; 10 USC 1104, Sharing of Healthcare Resources with the Department of Veterans Affairs; 38 USC 8111, Sharing of Department Veterans Affairs and Department of Defense Health Care Resources; National Defense Authorization Act (NDAA) 2017, Defense Health Programs; 10 USC 136, Under Secretary of Defense for Personnel and Readiness; 10 USC 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); DoD Instruction (DODI) 6025.18, Privacy of Individually Identifiable Health Information in DoD Health Care Programs; DoD Regulation 6025.18-R, DoD Health Information Privacy Regulation; DoDI 6040.45, DoD Health Record Life Cycle Management; DoDI 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFs); and EO 9397 (SSN), as amended.

PURPOSE: To provide and document your medical care; determine 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.

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 non-government 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 non-government organizations to perform DoD-approved research. Information in your records may be used for other lawful reasons including teaching, compiling statistical data, and evaluating the care rendered. Use and disclosure of your records outside of DoD may also occur per 5 USC 552a(b) of the Privacy Act of 1974, as amended. Protected health information (PHI) in your records may be used and disclosed 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.

APPLICABLE SORN: EDHA 07, Military Health Information System (June 15, 2020, 85 FR 36190)
<https://dpcl.d.defense.gov/Portals/49/Documents/Privacy/SORNS/DHA/EDHA-07.pdf>

DISCLOSURE: 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.

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)

<input checked="" type="checkbox"/> Within the DoD Component	Specify.	DHMSM PMO and Joint Operational Medicine Information System (JOMIS)
<input checked="" type="checkbox"/> Other DoD Components (i.e. Army, Navy, Air Force)	Specify.	Army, Navy, and Air Force MTFs
<input checked="" type="checkbox"/> Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)	Specify.	VA, Department of Health and Human Services (HHS), Social Social Administration (SSA), and USCG within the U.S. Department of Homeland Security (DHS)
State and Local Agencies	Specify.	

Leidos Partnership for Defense Health (LPDH). The contract Performance Work Statement (PWS) paragraph 5.1.10.12 and sub-paragraphs serve as required Business Associate Agreement (BAA).

The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect Government data. The Contractor shall also ensure the confidentiality, integrity, and availability of Government data in compliance with all applicable laws and regulations, including data breach reporting and response requirements, in accordance with Defense Federal Acquisition Regulation (DFAR) Supplement, Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoDD 5400.11, "DoD Privacy Program," May 8, 2007, and DoD 5400.11-R, "DoD Privacy Program," May 14, 2007. The Contractor shall also comply with federal laws relating to freedom of information and records management.

The TRICARE Management Activity (TMA) Privacy Office website at <http://www.tricare.mil/tmaprivacy/contract.cfm> contains guidance regarding PHI/PII.

PII is shared with systems hosted on Amazon Web Services (AWS), but AWS does not have access to the encrypted data stored on its cloud services. AWS is an accredited cloud service provider per FedRAMP and DoD Cloud SRG guidance, and is subject to DFARS Case 2013-D018 directly under DoD guidance via DISA provisional authorization.

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. RevSpring, SSI Group, Experian, and Alpha II

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

Existing DoD Information Systems: DHMSM EHR systems within the DoD; legacy EHR systems from Armed Forces Health Longitudinal Technology Application (AHLTA) and Composite Health Care System (CHCS) via Defensive Medical Information Exchange (DMIX) systems within the DoD; and Theater Medical Data Store (TMDS) within the DoD

Other Federal Information Systems: VA EHR system, Veterans Health Information Systems and Technology Architecture (VistA) within the VA; - Medicare and Medicaid benefits information from information systems within HHS; and Patient identity and mortality status information from Death Master File (DMF) system within the Social Security Administration (SSA)

Commercial Systems include RevSpring, SSI Group, Experian, and Alpha II.

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)

Patient information is also collected via the portal and the following forms: DD2870; DD2871; DD2569; OF522; DD2005; Notice of Privacy Practices; MHS GENESIS Patient Portal web site < <https://patientportal.mhsgenesis.health.mil> >

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 EDHA 07

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

I. 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. **Unscheduled**

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

(3) Retention Instructions.

Unscheduled - Permanent. Treat system and/or records maintained in the system as permanent until a NARA approved schedule and disposition authority has been applied.

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 statute 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.

10 USC 8111, Sharing of Department of VA and DoD Healthcare Resources; 10 USC 1104, Sharing of Healthcare Resources with the Department of Veterans Affairs; 38 USC 8111, Sharing of Department Veterans Affairs and Department of Defense Health Care Resources; National Defense Authorization Act (NDAA) 2017, Defense Health Programs; 10 USC 136, Under Secretary of Defense for Personnel and Readiness; 10 USC Chapter 55, Medical and Dental Care; 42 USC 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 6025.18, Privacy of Individually Identifiable Health Information in DoD Health Care Programs; DoDI 6025.18-R, DoD Health Information Privacy Regulation; DoDI 6040.45, DoD Health Record Life Cycle Management; DoDI 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFs); and EO 9397 (SSN), as amended.

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.

OMB Collection Title: MHS GENESIS Patient Registration Module & Patient Portal; OMB Control Number: 0720-0064; Expiration Date: 10.31.22