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:

MHS-GENESIS - Electronic Health Record (MHS GENESIS - EHR)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

10/08/24

Defense Healthcare Management System Modernization (DHMSM) Program Management Office

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 Military Health System (MHS) GENESIS Electronic Health Record (EHR) is a collection of integrated and interdependent subsystems which collectively comprise 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). The EHR System collects, processes, and distributes EHR longitudinally across the Military Health System (MHS), Department of Veterans Affairs (VA) and other Federal agencies enabling the application of standardized workflows, integrated healthcare delivery, and data standards for improved and secure electronic exchange of medical and patient data between the DoD and its external partners, including the Department of Veterans Affairs (VA) and private sector healthcare providers. MHS GENESIS consists of the following subsystems:

MHS GENESIS Infrastructure provides the core networking services and shared tools/services for MHS GENESIS; EHR Core is the primary clinical suite of software for MHS GENESIS designed to unify and increase accessibility of integrated, evidence-based healthcare delivery and decision-making; MHS GENESIS High Assurance Clinical Application Services (HA-CAS) provides additional solutions to EHR Core suite of applications, Patient Portal, HealtheIntent, CAMM7, Dragon Nuance, Health Information Exchange (HIE), Cloud IAM and Millennium Cloud Services; MHS GENESIS Test provides a testing environment for MHS GENESIS; MHS GENESIS Train is the training environment for MHS GENESIS users; MHS GENESIS Build provides an environment for dedicated wave deployment, specifically the enterprise build, localized build and testing, in use by Initial Operating Capacity developers and local site experts engaged in deployment activities, including design and configuration Workshops (National and Local), System Validation Sessions and Integration Validation.

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). Categories of individuals whose information is stored in this system include: active-duty military (all services + Reserve), Coast Guard, National Guard, dependents, retirees and/or their dependents, contractors, veterans, and other categories of individuals eligible to receive care at Federal Treatment Facilities.

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 a variety of uses, both mission-related and administrative. Primarily, the PII is required for patient identification, verification, and authentication in the course of scheduling and administering medical treatment. Additionally, the PII could be used 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? [x] 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 compliant 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? [X] 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.)*

[X] 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 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); DoD Instruction 6025.18, Privacy of Individually Identifiable Health Information in DoD Health Care Programs; DoD Regulation 6025.18-R, DoD Health Information Privacy Regulation; DoD Instruction 6040.45, DoD Health Record Life Cycle Management; DoD Instruction 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFs); and E.O. 9397 (SSN), as amended.

PURPOSE: To collect information required to provide and document your medical care; determine your eligibility for benefits and entitlements; adjudicate claims; determine third party responsibility 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 which may include teaching, compiling statistical data, and evaluating the care rendered. Use and disclosure of your records outside of DoD may also occur in accordance with 5 USC 552a(b) of the Privacy Act of 1974, as amended.

Any protected health information (PHI) in your records may be used and disclosed generally 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://dpcld.defense.gov/Portals/49/Documents/Privacy/SORNs/DHA/EDHA-07.pdf

DISCLOSURE: Voluntary. Failure 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)*

[X] Within the DoD Component	Specify.	Joint Operational Medicine Information System (JOMIS), and Enterprise Intelligence and Data Solutions (EIDS)
[X] Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Army, Navy, and Air Force MTFs
[X] Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	VA, Department of Health and Human Services (HHS), Social Social Administration (SSA) USCG within the U.S. Department of Homeland Security (DHS), National Security Agency (NSA), National Oceanic and Atmospheric Administration (NOAA)
[ ] State and Local Agencies	Specify.	

[X] 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.	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 following language is contained in the contract per Defense Federal Acquisition Regulation (DFAR) Supplement, Subpart 224.1 (Protection of Individual Privacy), which incorporates DoD 5400.11, and DoD 5400.11-R. The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect Government data. The Contractor shall ensure the confidentiality, integrity, and availability of Government data per applicable laws and regulations, including data breach reporting and response requirements, per DFAR Supplement, Subpart 224.1 (Protection of Individual Privacy). The Contractor shall comply with federal laws and records management. PII is shared with systems hosted on Amazon Web Services (AWS), however, 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 their DISA provisional authorization.
[X] 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)*

- [X] Individuals
- [ ] Databases
- [X] Existing DoD Information Systems
- [X] Commercial Systems
- [X] Other Federal Information Systems

Existing DoD Information Systems:- Patient identity, service status, immunization, and benefits information from Defense Manpower Data Center via MHS-GENESIS EHR systems within the DoD;- Continuity of care information from 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- Operational Medicine data from Theater Medical Data Store (TMDS) within the DoD

Other Federal Information Systems:- Coordination and continuity of care information from 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: RevSpring, SSI Group, Experian, and Alpha II (Patient statements and insurance claim data)

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

- [ ] E-mail
- [X] Official Form (*Enter Form Number(s) in the box below)*
- [X] In-Person Contact
- [ ] Paper
- [ ] Fax
- [X] Telephone Interview
- [X] Information Sharing - System to System
- [X] Website/E-Form
- [X] 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.

[X] 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://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.

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.

N1-330-10-003, DAA-GRS-2017-0010-0009, NC1-330-77-004, DAA-GRS-2017-0010-0001, DAA-GRS-2022-0009-0001, DAA-0330-2014-0014-0001, DAA-GRS-2013-0006-0003, DAA-GRS-2013-0005-0003

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

(3) Retention Instructions.

Note: Please refer to NARA approved, pending, or GRS authority and retention instruction specific to each sub systems, applications, electronic collections, file servers, and share drives for each system.

MHS-GENESIS Records retention:

FILE NUMBER: 927-01, Armed Forces Military Service Treatment Record (STR)
DISPOSITION: Temporary. Cut off after the date of separation of the member from the Armed Services. Destroy 100 years after cutoff.

FILE NUMBER: 927-02, Outpatient Records of Retired/Family Members/NATO/Non-NATO Foreign National/Army ROTC, Army Reserve, Army National Guard on training of less than 30 days/Others (NSTR)
DISPOSITION: Temporary. Cut off after the end of the calendar year of the last date of treatment. Retire to the National Personnel Records Center (NPRC) two years after cutoff. Destroy 50 years after cutoff.

FILE NUMBER: 202-26.2, Dept of Defense Civilian Employee Occupational Individual Medical Case Files – Long-Term Records (OHTR)
DISPOSITION: Temporary. Cut off upon separation of employee or when the Official Personnel File (OPF) is destroyed, whichever is later. Destroy 30 years after cutoff. NOTE: When an employee transfers to another Federal agency, the long-term Occupational Individual Medical Case Files must be transferred to the gaining agency at the same time as the employee's OPF per 5 CFR 293, Subpart E -§293.510(a).

FILE NUMBER: 927-04, Inpatient, Extended Ambulatory Records and Fetal Monitoring Strips – Military Treatment Facilities
DISPOSITION: Temporary. Cut off after the end of the calendar year of the completion of the records or upon closure of treatment center MTF or rotation to another military department, whichever is first. Retire to the National Personnel Records Center (NPRC), return to parent unit medical record department, or hold in theater holding area no later than 1 year after cutoff. Destroy 50 years after cutoff.

FILE NUMBER: 927-09, Substance Abuse Records
DISPOSITION: Temporary. Cut off after the end of the calendar year the case is closed. Destroy 5 years after cutoff or when minor child reaches 23 years old, as applicable.

FILE NUMBER: 927-10, Mental Health Records
DISPOSITION: Temporary. Cut off after the end of the calendar year the case is closed. Destroy 5 years after cutoff or when minor child reaches 23 years old, as applicable.

FILE NUMBER: 927-11, Entrance and Separation X-ray Films
DISPOSITION: Temporary. Cut off and retain x-rays, along with all additional films taken as a result of questionable anomalies that do not result in an applicant being rejected, no longer than 4 months after creation. Retire x-ray film to NPRC 111 Winnebago Street, St Louis, MO. 63118. VA is authorized custodian of records after transfer (VA schedule RCS VB-1, Part 1, Section XIII (13-061.100)). Destroy in accordance with current VA disposition instructions.

FILE NUMBER: 927-16, Routine Employment X-ray Films (not related to Occupational Illness, Injury or Accident) on Civilian Employees

DISPOSITION: Temporary. Cut off after date of last film. Destroy 5 years after cutoff.

FILE NUMBER: 927-19, Mammograms/Breast Ultrasound
DISPOSITION: Temporary. Cut off after the end of the calendar year in which the last film was taken. Destroy 10 years after cutoff.

FILE NUMBER: 927-20, Radiation Oncology Films
DISPOSITION: Temporary. Cut off after the end of the calendar year in which the last film was taken. Destroy 15 years after cutoff.

FILE NUMBER: 927-23, Family Advocacy Case Records - Substantiated Cases and Unsubstantiated-Unresolved Cases
DISPOSITION: Temporary. Cut off after the end of the calendar year in which the case review committee determination was made or treatment ends. Retire to the NPRC (MPR) National Personnel Record Center, 9700 Page Blvd., St. Louis, MO 63132, 2 years after cutoff. Destroy as a family group 25 years after cutoff.

FILE NUMBER: N/A, Blood Records
DISPOSITION: Unscheduled. Maintain permanently until an approved NARA disposition authority is applied.

FILE NUMBER: 201-14, Staffing Surveys and Studies Files
DISPOSITION: Temporary. Cut off annually. Destroy 5 years after cutoff.

FILE NUMBER: 1919-02, Clinic (Health Unit) Scheduling Records
DISPOSITION: Temporary. Cut off annually. Destroy 3 years after cutoff.

FILE NUMBER: N/A, Coding Compliance
Disposition: Unscheduled. Maintain permanently until an approved NARA disposition authority is applied.

FILE NUMBER: 103-13, Transitory Records
DISPOSITION: Temporary. Cut off and destroy when no longer needed for business use.

FILE NUMBER: 911-01, TRICARE Contractor Claims Records
DISPOSITION: Temporary. Cut off at end of the calendar year in which received. Destroy 10 years after cutoff.

FILE NUMBER: 1601-02, System Access Records - Systems not requiring Special Accountability for Access
DISPOSITION: Temporary. Cut off and destroy when business use ceases.

FILE NUMBER: 1601-12, Data Administration and Documentation - Temporary Systems
DISPOSITION: Temporary. Cut off after the project/activity/transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system. 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.

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); DoD Instruction 6025.18, Privacy of Individually Identifiable Health Information in DoD Health Care Programs; DoD 6025.18-R, DoD Health Information Privacy Regulation; DoD Instruction 6040.45, DoD Health Record Life Cycle Management; DoD Instruction 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.

The information collected in this system is for the diagnosis and treatment of medical conditions and is not considered a public information collection per DoDM 8910.01, V2, Encl 3, paragraph 8b(5).