**SYSTEM NAME AND NUMBER:** Military Health Information System, EDHA 07. (June 15, 2020; 85 FR 36190)

**SECURITY CLASSIFICATION:** Unclassified.

**SYSTEM LOCATION:** Defense Health Agency (DHA), Electronic Health Records (EHR) Core Program Office, 7700 Arlington Boulevard, Falls Church, VA 22042-510.

**SYSTEM MANAGER(S):** Program Manager, EHR Core Program Office, 1700 N Moore Street, Suite 2300, Arlington, VA 22209. dha.ncr.peo-ipo.mbx.peo-dhms-communications@mail.mil.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** Public Law 104-191, Health Insurance Portability and Accountability Act of 1996; 10 U.S.C., Chapter Ch. 55, Medical and Dental Care; 10 U.S.C. 1097a, TRICARE Prime: Automatic Enrollments; Payment Options; 10 U.S.C. 1097b, TRICARE Prime and TRICARE Program: Financial Management; 10 U.S.C. 1079, Contracts for Medical Care for Spouses and Children: Plans; 10 U.S.C. 1079a, TRICARE Program: Treatment of Refunds and Other Amounts Collected 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; 10 U.S.C. 1095, Health Care Services Incurred on behalf of Covered Beneficiaries: Collection From Third-party Payers; 42 U.S.C. 290dd, Substance Abuse Among Government and Other Employees; 42 U.S.C. 290dd-2, Confidentiality Of Records; 42 U.S.C 42 U.S.C. Ch. 117, Sections 11131-11152, Reporting of Information; 45 CFR 164, Security and Privacy; Department of Defense (DoD) Instruction 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFS); DoD 6025.18-R, DoD Health Information Privacy Regulation; and E.O. 9397 (SSN).

**PURPOSE(S) OF THE SYSTEM:** The MHIS collects and maintains data that supports benefits determination for Military Health System (MHS) beneficiaries between DoD, Department of Veterans Affairs (VA), and Department of Health and Human Services (HHS) healthcare programs. The MHIS collects and maintains data used to authenticate and identify American Red Cross volunteers and United Service Organizations granted privileges and access to DoD facilities. This data provides Federal Agencies the ability to support continuity of care for patrons, ensures more efficient adjudication of claims, enables quality assurance and healthcare operations, and supports a myriad of healthcare policy, public health, military mission, data analysis, and clinical research activities. The system documents and tracks environmental health data, deployment information, and data used to perform disease management. The system also maintains data used in proactive health intervention activities. Data is used for research and data analysis to support military missions, improve safety, and advance military technology. Continuity of care includes maintaining data for patient administration (including registration, admission, disposition and transfer); patient appointments and scheduling delivery of managed care; workload and medical services accounting; and quality assurance. Data collected and maintained is also used to capture demographics and perform trend analysis.

The information stored in this system consists of personally identifiable information (PII) protected by the Privacy Act and personal health information (PHI) protected by the Health Insurance Portability and Accountability Act (HIPAA). The DoD Health Information Privacy Regulation (DoD 6025.18-R) issued pursuant to the HIPAA of 1996, applies to most health information. DoD 6025.18-R may place additional procedural requirements on the uses and disclosures of such information beyond those found in the Privacy Act of 1974 or mentioned in this System of Records Notice (SORN).

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** Members, former members, retirees, civilian employees (includes non-appropriated fund) and contractor employees of the DoD and all of the Uniformed Services; Presidential appointees of all Federal Government agencies; Medal of Honor recipients; U.S. Military Academy students; Lighthouse Service, DoD and VA beneficiaries (e.g. dependent family members, legal guardians and other protectors, prior military eligible for VA benefits, Non-DoD Beneficiary and DoD Beneficiary, a person who receives benefits from the DoD based on prior association, condition or authorization, an example is a former spouse; Former member (Reserve service, discharged from Ready Reserve or Selective Reserve following notification of retirement eligibility); non-Federal agency civilian associates and other individuals granted DoD privileges, benefits, or physical or logical access to military installations (e.g., American Red Cross paid employees, United Service Organization (USO), Intergovernmental Personnel Act Employees (IPA), Boy and Girl Scout Professionals, non-DoD contract employees); members of the public treated for a medical emergency in a DoD or joint DoD/VA medical facility; Non-DoD Civilian employee; and individuals requiring a Common Access Card to access DoD information technology applications (i.e., Department of Homeland Security employees, state National Guard Employees, and Affiliated Volunteers); Civilian Retirees; DoD Outside of the Continental United States (OCONUS) Hires; Foreign Army; Foreign Navy; Foreign Marine Corps; Foreign Air Force; and Foreign Coast Guard.

**CATEGORIES OF RECORDS IN THE SYSTEM:** Eligibility and Enrollment Data: Selected electronic data elements extracted from the Defense Enrollment Eligibility Reporting System (DEERS) regarding personal eligibility for and enrollment in various health care programs within the DoD and among DoD and other federal healthcare programs including those of the VA, the HHS, and contracted health care provided through funding provided by one of these three Departments. Personal data includes: Name; DoD ID number; Social Security Number (SSN); address; email address(es); date of birth; gender; branch of service; citizenship; DoD Benefits number; DEERS ID number; sponsorship and beneficiary information; race and ethnic origin; religious preference;

Emergency Data information may include spouse's name and address; children's names, dates of birth, address and telephone number; parents' names, addresses and telephone numbers; or emergency contact's name and address;

Employment Information: Employment status; duty position; email address(es); leave balances and history; work schedules; individual personnel records; time and attendance records; retirement records, sponsor duty location, unit of assignment; occupation; rank; skill specialty; security clearance information.

Personal Financial Information: Pay, wage, earnings information; separation information; financial benefit records; income tax withholding records; accounting records.

Medical Readiness and Deployment Information: Inpatient and outpatient medical records; diagnosis codes; admission and discharge dates; location of care; pharmacy records; immunization records; Medical and Physical Evaluation Board records; neuropsychological functioning and cognitive testing data; periodic and deployment-related health assessments.

Clinical Encounter Data: Electronic data regarding beneficiaries' interaction with the MHS including health care encounters, health care screenings and education, wellness and satisfaction surveys, and cost data relative to such healthcare interactions. Electronic data regarding Military Health System beneficiaries' interactions with the VA or HHS healthcare delivery programs where such programs effect benefits determinations between these Department-level programs, continuity of clinical care, or effect payment for care between Departmental programs inclusive of care provided by commercial entities under contract to these three Departments.

Electronic data regarding dental tests, pharmacy prescriptions and reports, data incorporating medical nutrition therapy and medical food management, data for young MHS beneficiaries eligible for services from the military medical departments covered by the Individuals with Disabilities Educations Act (IDEA). Data collected within the system also allows beneficiaries to request an accounting of who was given access to their medical records prior to the date of request. It tracks disclosure types, treatment, payment and other Health Care Operations (TPO) versus non-TPO, captures key information about disclosures, process complaints, process and track request for amendments to records, generates disclosure accounting and audit reports, retains history of disclosure accounting processing. The Protected Health Management Information Tool (PHMIT), an electronic disclosure-tracking tool, assists in complying with the HIPAA Privacy disclosure accounting requirement. The PHIMT stores information about all disclosures, complaints, authorizations, restrictions and confidential communications that are made about or requested by a particular patient.

Occupational and Environmental Exposure Data: Electronic data supporting exposure-based medical surveillance; reports of incidental exposures enhanced industrial hygiene risk reduction; improved quality of occupational health care and wellness programs for the DoD workforce; hearing conservation, industrial hygiene and occupational medicine programs within the MHS; and timely and efficient access of data and information to authorized system users.

**RECORD SOURCE CATEGORIES:** Individuals; all DoD databases flowing into or accessed through the following integrated data systems, environments, applications, and tools: The Composite Health Care System (CHCS) and individual Service readiness applications, contractor systems providing clinical results, personnel systems, workload management systems; Defense Manpower Data Center, other developers (Lab Corp, Quest and EpiLab to perform patient specimen laboratory testing); DEERS; and all other systems within the DoD systems' repository that meets the regulatory requirements of this System of Records notice collection. Military Departments' medical treatment facilities, Medical Centers and Hospitals: Uniformed Services Treatment Facilities, and commercial healthcare providers; HHS; VA, and any other source financed through the Defense Health Program.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:** In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government when necessary to accomplish an agency function related to this System of Records.

b. To permit the disclosure of records to the HHS and its components, other federal agencies, and academic institutions for the purposes of public health activities and conducting research, including to facilitate collaborative research activities.

c. To the Congressional Budget Office for projecting costs and workloads associated with DoD Medical benefits.

d. To the VA for the purpose of providing medical care to former service members and retirees, to determine the eligibility for or entitlement to benefits, to coordinate cost sharing activities, and to facilitate collaborative research activities between the DoD and VA.

e. To the National Research Council, National Academy of Sciences, National Institutes of Health, Armed Forces Institute of Pathology, and similar institutions for authorized health research in the interest of the Federal Government and the public.

f. To local and state government and agencies for compliance with local laws and regulations governing control of communicable diseases, preventive medicine and safety, child abuse, and other public health and welfare programs.

g. To federal offices and agencies involved in the documentation and review of defense occupational and environmental exposure data.

h. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

i. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

j. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

k. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

l. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

m. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the System of Records; (2) the DoD determined as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

n. To another Federal agency or Federal entity, when the DoD determines information from this System of Records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:** Electronic and paper.

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:** Name, SSN, Beneficiary ID (sponsor's ID, patient's name, patient's DOB, and family member prefix or DEERS dependent suffix), diagnosis codes, admission and discharge dates, location of care or any combination of the above.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:** Temporary. Cut off upon last episode of patient care or last entry to the patient record is annotated. Delete/Destroy when 75 years old.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:** Multifactor log-in authentication including CAC authentication and password. Access controls enforce need-to-know policies so only authorized users have access to PII and/or PHI. Additionally, security audit and accountability policies and procedures directly support privacy and accountability procedures. Network encryption protects data transmitted over the network while disk encryption secures the disks storing data. Key management services safeguards encryption keys. Sensitive data is identified and masked as practicable. All individuals granted access to this System of Records must complete requisite training to include Information Assurance and Privacy Act training. Sensitive data will be identified, properly marked with access by only those with a need to know, and safeguarded as appropriate.

**RECORD ACCESS PROCEDURES:** Individuals seeking access to information about themselves contained in this System of Records should address written inquiries to the Chief, Freedom of Information Act (FOIA) Service Center, Defense Health Agency, Privacy and Civil Liberties Office, 7700 Arlington Boulevard, Suite 5101, Falls Church, VA 22042-5101.

Written requests for information should include the individual's full name, home address, home phone number, and SSN/DoD ID number, the identifier of this SORN, and signature. If requesting information about a legally incompetent person, the request must be made by the legal guardian or person with legal authority to make decisions on behalf of the individual. Written proof of that status may be required before any records will be provided. In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

**CONTESTING RECORD PROCEDURES:** The DoD rules for accessing records, for contesting contents and appealing initial agency determinations are published in 32 CFR part 310, or may be obtained from the system manager.

**NOTIFICATION PROCEDURES:** Individuals seeking to determine whether information about themselves is contained in this System of Records should address written inquiries to Chief, Freedom of Information Act (FOIA) Service Center, Defense Health Agency, Privacy and Civil Liberties Office, 7700 Arlington Boulevard, Suite 5101, Falls Church, VA 22042-5101.

Written requests should contain the individual's full name, home address, home phone number, and SSN/DoD ID number, the identifier of this SORN, and signature. If requesting information about a legally incompetent person, the request must be made by the legal guardian or person with legal authority to make decisions on behalf of the individual. Written proof of that status may be required before the existence of any information will be confirmed. In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:** None.

**HISTORY:** March 30, 2006, 71 FR 16127; November 18, 2013, 78 FR 69076.