

BILLING CODE: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-YYYY-HA**-XXXX]**

Privacy Act of 1974; System of Records

AGENCY: <Defense Health Agency, DoD>

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Defense (DoD) is modifying and reissuing a current system of records titled, <“Defense Medical Human Resource System internet (DMHRSi), EDHA 11.”> This system of records was originally established by the <Defense Health Agency> to collect and maintain records on <all of the human resources functions and permit ready access to manpower, personnel, readiness, labor cost assignment, and education and training information across the DoD medical enterprise. This system of records provides a single database source of instant query/access for all personnel types and readiness posture of all DoD medical personnel.> This system of records notice (SORN) is being updated to <to add additional “categories of records” that will be stored in the system.>. **DATES:** This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before [**INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**]. The Routine Uses are effective at the close of the comment period.

ADDRESSES: You may submit comments, identified by docket number and title, by either of the following methods:

* Federal Rulemaking Portal: <https://www.regulations.gov>. Follow the instructions for submitting comments.

* Mail: DoD cannot receive written comments at this time due to the COVID-19 pandemic.
Comments should be sent electronically to the docket listed above.

Instructions: All submissions received must include the agency name and docket number for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <https://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: < Insert name, title, office name, mailing and email address, and phone number of the Component privacy officer.>

SUPPLEMENTARY INFORMATION:

I. Background

The <*Defense Medical Human Resource System internet (DMHRSi), EDHA 11*> system of records is used to <*collect and maintain records on all of the human resources functions and permit ready access to manpower, personnel, readiness, labor cost assignment, and education and training information across the DoD medical enterprise. This system of records provides a single database source of instant query/access for all personnel types and readiness posture of all DoD medical personnel.*>. Subject to public comment, the DoD proposes to update this SORN to add the standard DoD routine uses (routine uses A through I). Additionally, the following sections of this SORN are being modified as follows ... <to the Categories of Records in the System section to add additional data elements that will be captured by the system.>

DoD SORNs have been published in the Federal Register and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Defense Privacy, Civil Liberties, and Transparency Division website at <https://dpclld.defense.gov/privacy>.

II. Privacy Act

Under the Privacy Act, a “system of records” is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and OMB Circular No. A-108, DPCLTD has provided a report of this system of records to the Office of Management and Budget (OMB) and to Congress.

Dated:

Aaron T. Siegel,
Alternate OSD Federal Register
Liaison Officer, Department of Defense.

NOTE: Within the system notice itself (below), do not rely on previously defined acronyms from the preamble; spell out everything anew and define the acronym again. This is because the preamble text does change as the SORN is amended each time, and previously defined acronyms may not be defined in any new preamble, leaving the public to wonder what the acronym is referring to. Also the SORN should stand on its own without reference to the preamble or background information in the Federal Register Notice.

SYSTEM NAME AND NUMBER: <Defense Medical Human Resource System internet (DMHRSi)>, <System Number 387>.

SECURITY CLASSIFICATION: <Unclassified>

SYSTEM LOCATION: < 5109 Leesburg Pike (Sky 6), Falls Church, VA 22041.>

SYSTEM MANAGER: The system manager is <Chief/Deputy Program Manager, Resources Division, Solutions Delivery Division, Defense Health Agency, 5109 Leesburg Pike (Sky 6), Falls Church, VA 22041>.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: <10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; E.O. 12656, Assignment of Emergency Preparedness Responsibilities; DoDD 5136.01, Assistant Secretary of Defense for Health Affairs (ASD(HA)); DoDI 1322.24, Medical Readiness Training; DoD 6010.13-M, Medical Expense Performance Reporting System for Fixed Military Medical and Dental Treatment Facilities Manual; and E.O. 9397 (SSN), as amended.>

PURPOSE(S) OF THE SYSTEM: <To consolidate all of the human resources, functions and permit ready access to manpower, personnel, readiness, labor cost assignment, and education and training information across the DoD medical enterprise. This system of records provides a single

database source of instant query/access for all personnel types and the readiness posture of all DoD medical personnel.>

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: <Active Duty Military, Reserve, National Guard, Civilian Employees who are assigned to or part of the Military Health System or the Defense Health Agency (DHA), and includes non-appropriated fund employees, DoD contractors, and volunteers.>

CATEGORIES OF RECORDS IN THE SYSTEM: <individual's name, date of birth, social security number (SSN), and /or DoD identification (ID) number, national provider identifier (NPI), personnel category code, token type code, token end calendar date, gender, place of birth, citizenship, home address, home telephone number, individual's personal mobile phone number for military readiness recall, business email address, work address, work telephone number, race/ethnicity, marital status, training and career certifications, medical training information including class names and class dates, military rank information, specialty, licensure, educational background, personnel security clearance data, common access card (CAC) information such as issue date, type, and end date, medical readiness training and other health information required to determine an individual's fitness to perform their duties.>

RECORD SOURCE CATEGORIES: Records and information stored in this system of records are obtained from: <DoD pay and personnel systems, the Defense Enrollment Eligibility Reporting System (DEERS), DoD medical facilities personnel, DoD supervisors, and DoD operational records.>

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,

all or a portion of the records or information contained herein 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 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.

C. 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.

D. 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 that 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.

E. 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.

F. 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.

G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines 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.

H. To another Federal agency or Federal entity, when the DoD determines that 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.

I. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

J. <The DoD Blanket Routine Uses set forth at the beginning of the Defense Privacy and Civil Liberties Division compilation of system of records notices may apply to this system. The complete list of DoD Blanket Routine Uses can be found online at:

<http://dpcl.d.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx>>

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, or digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and

Authorization Management Program (FedRAMP). *NOTE: Components may enhance with or substitute their preferred language as appropriate.*

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by <Individual's name and SSN and/or DoD ID number>.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained for <4 years. Cut off upon notification separation or termination from MHS assignment and/or employment. Destroy contractor, volunteer, and duplicate data on Active Duty, Guard, Reserve, and Federal Government employees from other military service electronic information systems 4 year(s) after cutoff.> and then destroyed.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: The DoD safeguards records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, the DoD established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. The DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including Common Access Card (CAC) authentication and password; Secret Internet Protocol Router (SIPR) token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who

will have access; identification, marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities. NOTE: *This is standard language used for the DoD-wide SORNs which Components may use as appropriate, or change or substitute as needed.*

RECORD ACCESS PROCEDURES: Individuals seeking access to their records should address written inquiries to the <the Chief, FOIA Service Center, Defense Health Agency Privacy and Civil Liberties Office, 7700 Arlington Boulevard, Suite 510, Falls Church, VA 22042-5101> FOIA Requester Service Center, Office of Freedom of Information, <insert website and address of the FOIA Office>. Signed written requests should contain the name and number of this system of records notice along with full name, **current address, and email address of the individual.** *If appropriate for the system of records, add additional data that is required or helpful, such as phone number, PII (such as DoD ID Number or Defense Benefits Number, date of birth), or case numbers as well.* In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the appropriate 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, contesting contents, and appealing initial Component determinations are contained 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 follow the instructions for Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: <“None.”>

HISTORY: <March 15, 2016, 81 FR 13779; November 19, 2014, 79 FR 68872; November 18, 2013, FR 69076; September 13, 2012, FR 56627; December 12, 2005, 70 FR 73454