PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Medical Human Resources System - Internet (DMHRSi)
Defense Health Agency (DHA)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☒ **Existing DoD Information System**
- ☐ **Existing Electronic Collection**
- ☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 130
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☒ **Yes**
- ☐ **No**

If "Yes," enter UPI UII: 007-000000611

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier EDHA11

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number	0720-0041
Enter Expiration Date	03/31/2015

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

5 U.S.C. 301, Departmental Regulations; DoD Directive 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 (MEPRS) for Fixed Medical and Dental Treatment Facilities; DoD 5136.1-P, Medical Readiness Strategic Plan (MHSP); E.O. 12656, Assignment of Emergency Preparedness Responsibilities; and E.O. 9397 (SSN), as amended.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Defense Medical Human Resources System - Internet (DMHRSi) is a web-based system that allows for enhanced management and oversight of the most important resource within the Department of Defense (DoD) — it's people. To support joint military operations, it is critical that military and civilian leadership have the most current information concerning all personnel; DMHRSi provides this visibility. DMHRSi has standardized the way human resources are tracked and managed across all service branches of the Military Health System (MHS) for all medical personnel from the services' entire military and civilian workforce.

DMHRSi enables consolidation of all Human Resources (HR) functions (i.e., essential manpower, personnel, labor cost assignment, education & training, and readiness information) including the following:

• Personnel in / out processing time greatly reduced.

• Provides tri-service standardized labor costing approach.

• Personnel have visibility of their own information.

• Provides instant visibility of assignment of projected gains / losses.

• Provides single database source of instant query / access for all personnel types and readiness posture of all personnel assigned to platforms.

• Allows for instant visibility of available training at command and across MHS, enables individuals to request training online (eliminating paper requests), and tracks historical training.

• Tracks readiness equipment / clothing issuance and medical / administration requirements.

• Reduces upper echelon queries due to their ability to view command data and provides visibility of staffing levels (required and actual).

DMHRSi is deployed to all Military Treatment Facilities (MTFs) and clinics worldwide (over 600 sites with 170,000 users worldwide). Defense Health Agency (DHA) owns and operates DMHRSi.

The system is accessible via a public web site across the Internet by anyone with the Uniform Resource Locator (URL). The system is not intended to be accessed by the general public; an individual must have an active .mil or .gov email account to access the web site and must have their account authenticated by a system administrator.

Should be revised to read:

Data is collected in DMHRSi from the following categories of individuals:
• Military Personnel (Active Duty, Reserve, Guard) for Army, Navy, Air Force,
• Borrowed Personnel as applicable from Coast Guard, Public Health Services, Local Nationals, Marines
• Federal Civilians (DoD, Army, Navy, Air Force, VA)
• Contractors
• Volunteer personnel

DMHRSi collects, maintains, transmits, and stores the following types of personally identifiable information (PII): personal descriptors, ID numbers, ethnicity, employment, life, and education information.

PII elements are used for identification in both input and output transactions. This practice is driven by the lack of unique identifiers in the external systems to which DMHRSi interfaces. The PII elements that are used typically are some combination of SSN, full name, and month of birth.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Privacy risks may include, but are not limited to, the following:

•Distribution of a password to an incorrect user;

•Incorrect password reset;

•Linking of log in ID to wrong account; and

•Criminal wrongdoing or misconduct.

In accordance with the DoD 5400.11-R, "Defense Privacy Program," May 14, 2007, whenever a DMHRSi user and/or DMHRSi support personnel becomes aware of an actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purpose where one or more individuals will be adversely affected, DMHRSi will:

• Notify appropriate leadership personnel within the DMHRSi Program Office immediately;

• Report to the United States Computer Emergency Readiness Team within one hour of breach discovery;

• Report to the DHA Privacy and Civil Liberties Office within 24 hours at PrivacyOfficerMail@dha.mil; and

• Notify all affected individuals within 10 working days after the loss, theft, or compromise is discovered and the identities of the individuals ascertained, if necessary.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. DHA

☒ **Other DoD Components.**

Specify. Inbound Interfaces:

• AUTODIN Automatic Maintenance Program System (AAMPS) – Monthly
• Defense Civilian Personnel Data System (DCPDS) – Weekly
• Defense Civilian Pay System (DCPS) – Weekly
• Manpower Programming and Execution System (MPES) – Weekly
• Military Personnel Data System (MILPDS) – Weekly
• Medical Operational Data System - Enlisted (MODSE) – Weekly
• Medical Operational Data System - Guard (MODSG) – Weekly
• Medical Operational Data System - Officer (MODSO) – Weekly
• Medical Operational Data System - PROFIS (MODSP) – Weekly
• Medical Operational Data System - Reserve (MODSR) – Weekly
• Navy Enlisted System (NES) – Weekly
• Occupational Database (ODB) – Quarterly
• Officer Personnel Information System (OPINS) – Weekly
• Navy Reserve System - Enlisted (RHSE) – Weekly
• Navy Reserve System - Officer (RHSO) – Weekly
• Table of Authorizations and Distributions System (TAADS) – Yearly

Outbound Interfaces:

• Expense Assignment System (EAS) – Monthly
• Enterprise-Wide Provider Data (EWPD) – Daily

Bi-Directional Interface:
• MHS Learn – Weekly
• DTMS – Weekly
• Navy Training Management and Planning System (NTMPS) – Weekly

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. CGI Federal, Planned Systems International (PSI), Aderas

Contract Language:

"The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data, to ensure the confidentiality, integrity, and availability of Government data."

"The contractor shall comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (P.L. 104-191) requirements, specifically the administrative simplification provisions of the law, as well as the Department of Defense (DoD) 6025.18-R, "DoD Health Information Privacy Regulation," January, 2003. This includes the Standards for Electronic Transactions, the Standards for Privacy of Individually Identifiable Health Information and the Security Standards. It is expected that the contractor shall comply with all HIPAA-related rules and regulations as they are published and as DHA requirements are defined (including identifiers for providers, employers, health plans, and individuals, and standards for claims attachment transactions)."

"The contractor will comply with the requirements in Office of Management and Budget (OMB) Circular A-130, in the DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007, and in the DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007."

☒ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Pursuant to local MTF policies, forms may or may not be used to collect an individual's PII. MTF personnel manually enter contractors' and volunteers' PII directly into DMHRSi.

(2) If "No," state the reason why individuals cannot object.

j. 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.

Consent to the specific uses of PII is obtained as necessary in accordance with DoD 5400.11-R, Department of Defense Privacy Program, C.4.1.3.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.	Most of the data collected in DMHRSi comes through formal data interfaces via DoD-controlled networks from DoD and Service / Federal personnel systems. However, PII on contractors and volunteers which is not in Federal personnel systems is collected at the Military Treatment Facility level by DMHRSi technicians authorized to enter the information into DMHRSi.

Prior to a user reaching a log on screen, the DMHRSi website displays a Privacy Act Warning and a HIPAA Warning, which are warnings to a system user, not to an individual whose PII is being collected. Because, in the case of some contractors and volunteers, PII for DMHRSi is collected directly from an individual, the following Privacy Act Statement should be used in connection with direct collection of PII from an individual:

Privacy Act Statement
This statement serves to inform you of the purpose for collecting your personal information and how it will be used.

AUTHORITY: 5 U.S.C. 301, Departmental Regulations; DoD Directive 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 (MEPRS) for Fixed Medical and Dental Treatment Facilities; DoD 5136.1-P, Medical Readiness Strategic Plan (MHSP); E.O. 12656, Assignment of Emergency Preparedness Responsibilities; and E.O. 9397 (SSN), as amended.

PURPOSE: Information is collected from military, civilian, contractor, and volunteer medical personnel in the Armed Services and throughout the Military Health System (MHS) in order to determine an individual's fitness to perform medical personnel duties and to assess medical personnel readiness of the Armed Services and the MHS. The information is also collected to support the medical personnel human resources functions of manpower, personnel, labor cost assignment, education, training, and readiness.

ROUTINE USES: Your records may be disclosed outside of DoD in accordance with the DoD Blanket Route Uses published at http://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx and as permitted by the Privacy Act of 1974, as amended (5 U.S.C. 552a(b)).

DISCLOSURE: Voluntary. If an individual refuses to provide information, no penalty may be imposed. However, failure to furnish requested information may result in administrative delays.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.