

## 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:

Military Health Systems (MHS) Information Platform (MIP)

### 2. DOD COMPONENT NAME:

Defense Health Agency

### 3. PIA APPROVAL DATE:

08/23/22

Program Executive Office Defense Healthcare Management Systems

### 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 Military Health Systems (MHS) Information Platform (MIP) is a system containing multiple dashboards and databases that deliver enterprise clinical data capabilities. The capabilities provided by MIP are: Program Management; Data Warehousing; Application Portal; Infrastructure and Operations; Application Support; Business Intelligence; Analytics; Predictive Analytics; Legacy Data Consolidation Service; Defense Medical Surveillance System; and Corporate Executive Information System. Types of projects enabled by MIP include clinical dashboards, reports, data feeds, ad-hoc data requests, a data mart, medical history tracking of individual service members, and identification of service members at elevated risk of injury or mental health illness.

MIP servers contain and process military medical data for use in data analysis and patient care. They deliver information to aid decision makers both at the military treatment facility level and at the enterprise management level. This capability subsequently provides an enhanced level of care for the Department of Defense; as well as other authorized individuals seeking medical treatment and interaction within the Military Health System. As a component of the MIP enclave, the Department of Defense and Department of Veterans Affairs Infrastructure for Clinical Intelligence (DAVINCI) is included in the enclave's Authority to Operate (ATO) and contains a subset of data from the enclave and VA's Corporate Data Warehouse (CDW). DAVINCI combines data from a population subset of data already stored in the MIP and connects to the VA's CDW (SORN 172VA10A7; August 25, 2020, 85 FR 52415).

Organizational Incident Operational Nexus (ORION) is one of the dashboards built into MIP used to track active duty Navy and Marine Corps service members who are exposed to traumatic events. ORION helps identify and track service members who are at an elevated risk for mental health injury so that ORION Outreach Coordinators can reach out to these service members with the goal of connecting them to mental health services, if desired. Service member contact information, medical history, major life stressors, and demographic information is used by ORION Outreach Coordinators to identify and contact service members who are higher risk, and by the ORION dashboard for predictive analysis.

The types of personal information about individuals contained in these systems include personally identifiable information (PII) and protected health information (PHI) such as name, date of birth, Armed Forces Qualification Test (AFQT) score, work history, Unit Identification Code, contact information, medical history and diagnoses, social supports, major life stressors, social security number (SSN), and other unique identifiers. Some information that includes PII will be coming directly from the patient.

The category of individuals includes anyone seen for treatment in any military treatment facility to include all Department of Defense active duty military, dependents, retirees, and retirees dependents. There may also be rare instances of others included if, for example if they were treated for emergent care in a military treatment facility.

The owner and manager of MIP is the Program Executive Office Defense Healthcare Management Systems (PEO DHMS), Enterprise Intelligence and Data Solutions Program Management Office (EIDS PMO).

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)

PII is collected for verification and identification of beneficiaries of DHA. This PII is for mission-related use and must be collected in order to deliver MIP's analytics capabilities to MIP users.

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 opportunity for individuals to object to the collection of PII is specific to the method used to collect PII in the respective information system and is addressed in the respective system's PIA. Additionally, during the MIP log in screen, patients have the opportunity to object to the collection of PII, by agreeing or disagreeing with disclosure statement.

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.

The opportunity for individuals to consent to uses of PII is specific to the method used by the respective information system and is addressed in the respective system's PIA. Additionally, during the MIP log in screen, patients have the opportunity to consent to the specific use of PII, by agreeing or disagreeing with disclosure statement.

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: 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; Public Law 104-191, Health Insurance Portability and Accountability Act of 1996; 10 U.S.C., Ch. 55, Medical and Dental Care; 42 U.S.C. 290dd-2, Confidentiality Of Records; 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 Manual 6025.18, Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs; and E.O. 9397 (SSN), as amended.

PURPOSE: The Military Health Systems Information Platform ("MHS MIP") contains multiple dashboards and databases that deliver enterprise clinical data capabilities, which may include, but are not limited to, verifying and identifying beneficiaries. It contains and processes military medical data for use in data analysis and to deliver information to aid decision makers at the military treatment facility level and enterprise management level.

ROUTINE USES: These records may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as follows: to contractors and others performing or working for the Federal Government when necessary to accomplish an agency function related to this System of Records; to the Department of Health and Human Services, other federal agencies, and academic institutions for the purposes of public health activities and conducting research; to the Department of Veteran's Affairs (VA) for the purpose of providing medical care, to determine the eligibility for benefits, to coordinate cost sharing activities, and to facilitate collaborative research activities between the DoD and VA; to the National Research Council and other similar institutions for authorized health research; and, among others, to federal offices and agencies involved in the documentation and review of defense occupational and environment exposure data. For a complete listing of the Routine Uses for this system, refer to the below hyperlinked SORN.

Any protected health information (PHI) in your records may be used and disclosed generally as permitted by the HIPAA Rules, as implemented within DoD. 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, there may be an administrative delay; however, care will not be denied and no penalties will be imposed.

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)

☒ Within the DoD Component

Specify. Defense Health Agency (DHA) and Military Treatment Facilities (MTFs)

☒ Other DoD Components (i.e. Army, Navy, Air Force)

Specify. Departments of the Army, Navy, and Air Force, as well as, Defense Manpower Data Center (DMDC).

☒ Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)

Specify.

Department of Veterans Affairs

☐ State and Local Agencies

Specify.

☒ 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.

N00178-14-D-7847, Parsons, Federal Acquisition Regulations (FAR) privacy clauses, i.e., 52.224-1 AND 52.239-1 Privacy Act of 1974, 36 CFR 119445 CFR Part 160, 162 and 164; 45 CFR Part 160, 162 and 164 Public Law 104-191; Public Law 104-191 DoDD 5400.7.

N65236-13-D-4943, DKW Communications, DoD 5220.22-M, SECNAVINST 5510.30, Privacy Act of 1974. FAR privacy clause 52.224-1.

N00178-14-D-7498, Task Order (TO)s N65236-18-F-3117 and N65236-19-F-3052, Spinsystems, Public Law 104-191 DoDD 5400.7; 45 CFR Part 160, 162 and 164; Privacy Act of 1974, Health Information Privacy and Accountability Act (HIPAA), Privacy Act Clause 52.224-1 and 52.224-2.

N00178-10-D-6093, TO N65236-19-F-3038, The Informatics Application Group (TIAG), Privacy Act of 1974, Health Information Privacy and Accountability Act (HIPAA), FAR privacy clause 52.224-1. CFR Part 160, 162 and 164 Public Law 104-191 36 CFR 119445 CFR Part 160, 162 and 164.

N00178-14-D-7490, TO N65236-18-F-3071, Sentar, FAR privacy clauses, i.e., 52.224-1. Privacy Act of 1974, HIPAA, 45 CFR Part 160, 162 and 164 Public Law 104-191. 36 CFR 119445 CFR Part 160, 162 and 164.

HT0015-17-C-0013, STS Systems Integration (SSI), PWS, 1.11.6 PII/PHI, Performance Work Statement (PWS), 5.3.4.2.22. PWS, Attachment 3, DHA Contractor NDA. PWS, Attachment 4, DHA ABM MAD Instructions for Contractor Access DoD IT Systems and CAC. Privacy Act of 1974. HIPAA

FA8052-16-C-0008, SPECPRO Management (SMS) SERVICES, PWS, 3.2.4. HIPAA, Public Law 104-191, DOD 6025.18-R. PWS, 3.2.5. Privacy Act, Public Law 100-503, DoDD 5400.11, DoD 5400.11-R. Broad Agency Announcements (BAA) PWS, APPENDIX A: HIPAA

HT0015-17-C-0008, SSI, PWS, 8 PII, PHI, and Federal Information Laws. Privacy Act of 1974, HIPAA

HT0015-17-C-0010, APPDDICTION STUDIO LLC, PWS, 6.1 PII, PHI and Federal Information Laws. PWS, 6.2, HIPAA. Privacy Act of 1974.

☐ Other (e.g., commercial providers, colleges).

Specify.

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-data is collected from sources and subsequently integrated into the MIP servers and databases. Source

systems include:

Artificial Intelligence Decompensation Expert Server (AIDEx)  
Armed Forces Health Longitudinal Technology Application (AHLTA)  
Aeromedical Service Information Management System (ASIMS)  
Carepoint Application Portal (CAP)  
Corporate Executive Information System (CEIS)  
Composite Health Care System (CHCS)  
Composite Occupational Health and Operational Risk Tracking (COHORT)  
Defense Medical Human resources System Internet (DMHRSi)  
Department of Defense Healthcare Management System Modernization (DHMSM)  
Defense Manpower Data Center (DMDC)  
Fleet Management & Planning System (FLTMPs)  
Legacy Data Consolidation Solution (MIP-LDCS)  
Marine Corps Total Force System (MCTFS)  
Navy Family Accountability and Assessment System (NFAAS)  
Pharmacy Data Transition Service (PDTs)  
Periodic Health Assessment (PHA)  
Post Deployment Health Assessment (PDHA)  
Surgical Scheduling System (S3)  
Total Workforce Management Services (TWMS)  
Data from Veterans Health Information Systems & Technology Architecture (VistA) is also integrated into MIP databases.  
Anesthesia Recording and Monitoring Device (ARMD)  
Medical Operational Data System (MODS)  
Medical Readiness Reporting System (MRRS)  
Navy Medicine Online (NMO)  
Clinical Information System (CIS)/Essentris  
MiCare  
National Intrepid Center of Excellence (NICoE)  
Remote Order Entry System (ROES)  
Corporate Data Warehouse (CDW)  
Defense Medical Surveillance System (DMSS)  
Defense Occupational and Environmental Health Readiness System – Hearing Conservation (DOEHRS-HC)  
Pharmacovigilance Defense Application System (PVDAS)  
DoD Trauma Registry (DoDTR)  
Enterprise Clinical Audiology Application (ECAA)  
Electronic Data Interchange (EDI) Humana  
HealthNet

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

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> E-mail   | <input type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input type="checkbox"/> In-Person Contact   | <input type="checkbox"/> Paper   |
| <input type="checkbox"/> Fax   | <input type="checkbox"/> Telephone Interview                                   |
| <input checked="" type="checkbox"/> Information Sharing - System to System                   | <input type="checkbox"/> Website/E-Form  |
| <input checked="" type="checkbox"/> Other (If Other, enter the information in the box below) |  |

MIP users have the option of voluntarily providing demographic information in the system (e.g. email).

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

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

(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.

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; Public Law 104-191, Health Insurance Portability and Accountability Act of 1996; 10 U.S.C., Ch. 55, Medical and Dental Care; 42 U.S.C. 290dd-2, Confidentiality Of Records; 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 Manual 6025.18, Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs; and E.O. 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.

Information obtained by the individual is considered minimal and does not require OMB approval.