

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 Information Platform Software Factory (MIP-SF)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

04/05/24

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.)

- | | |
|---|--|
| <input type="checkbox"/> From members of the general public | <input type="checkbox"/> From Federal employees |
| <input checked="" type="checkbox"/> from both members of the general public and Federal employees | <input type="checkbox"/> Not Collected (if checked proceed to Section 4) |

b. The PII is in a: (Check one.)

- | | |
|--|---|
| <input type="checkbox"/> New DoD Information System | <input type="checkbox"/> New Electronic Collection |
| <input checked="" type="checkbox"/> Existing DoD Information System | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> 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.

Military Health Systems Information Platform Software Factory (MIP-SF) is an enclave that hosts many applications, which are utilized via Container Runtime Environments (CRe). All software containers are deployed via the DevSecOps Community Cloud's (DSOCC's) Rancher Kubernetes Engines (RKEs) and hosted in AWS GovCloud.

Within MIP-SF, there is a solution known as the Data Exchange Service (DES), whose purpose is to offer a solution for health information exchange across organizations and to provide legacy health record data to systems that support clinical decisions and benefit adjudication. Its primary function is to serve as a back-end system that facilitates secure data exchanges between client and partner systems. DES is an integrated, Government Off-the-Shelf (GOTS) application that processes Personally Identifiable Information (PII), such as personal contact information, demographic information, employment information, and Protected Health Information (PHI) from active duty military personnel and/or qualifying personnel such as Federal employees and Federal contractors for administrative reasons.

The PII collected by DES-GC includes citizenship, home/cell phone, mailing/home address, place of birth, race/ethnicity, birth date, disability information, marital status, mother's middle/maiden name, personal email address, position/title, rank/grade, child information, DoD ID number, emergency contact information, medical information, names, other ID numbers, religious preference, SSN, and PHI (PHI collected includes radiology reports, vital signs, allergy records, immunization records, medications, diagnostic and lab results, clinical procedures, admission records, plan of care, problem lists, demographics, and insurance payer information). The categories of individuals on whom PHI/PII is collected include active duty military personnel and/or other qualifying personnel such as the spouse and dependents. DES then collates the data for provision to the health care provider.

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)

Within MIP-SF, DES uses PHI/PII for administrative, technical purposes to verify, identify, authenticate, and perform data matching to promote data sharing within DoD, VA, and other Federal Agencies and with participants of the eHealth Exchange.

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.

Individuals do not have the opportunity to object to the collection of their PII because MIP-SF is not the initial point of collection.

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.

Individuals do not have the opportunity to consent to the specific use of their PII because MIP-SF is not the initial point of collection.

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

MIP-SF does not collect PII directly from individuals. Therefore, no Privacy Act Statement or Privacy Advisory is required.

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.

DoD Medical Treatment Facilities (MTF's),
Defense Manpower Data Center (DMDC),
DoD Healthcare Management System Modernization
(DHMSM)

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

Specify.

Uniformed Services (Army, Air Force, Navy, Marines),
Family Support Services,
Defense Information Systems Agency (DISA)

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

Specify.

Department of Veterans Affairs (VA),
Social Security Administration (SSA)

State and Local Agencies

Specify.

Changes *** ASRC Federal Holding Company LLC,
Concept Plus LLC and Ward ENG Support Services
(WESSGRP) INC which manage and perform analysis of
the systems that stores the data neither send or receive any
PHI/PII.

In accordance with Defense Federal Acquisition Regulation
(DFAR) Supplement, Subpart 224.1 (Protection of
Individual Privacy), which incorporates by reference DoDD
5400.11, "DoD Privacy Program," May 8, 2007, and DoD
5400.11-R, "DoD Privacy Program," May 14, 2007.

Personally Identifiable Information (PII) and Protected
Health Information (PHI)

The Contractor shall establish appropriate administrative,
technical, and physical safeguards to protect any and all
Government data. The Contractor shall also ensure the
confidentiality, integrity, and availability of Government
data in compliance with all applicable laws and regulations,
including data breach reporting and response requirements,
in accordance with Defense Federal Acquisition Regulation
(DFAR) Supplement, Subpart 224.1 (Protection of
Individual Privacy), which incorporates by reference DoDD
5400.11, "DoD Privacy Program," May 8, 2007, and DoD
5400.11-R, "DoD Privacy Program," May 14, 2007. The
Contractor shall also comply with federal laws relating to
freedom of information and records management.

The DHA Privacy Office website at <https://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties> contains
guidance regarding PHI/PII.

AWS GovCloud (US) PII is shared with systems hosted on
Amazon Web Services (AWS), but 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.

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
 Existing DoD Information Systems
 Other Federal Information Systems

Databases
 Commercial Systems

Existing DoD Information Systems:

- Medical Operational Data System (MODS)
- Aeromedical Service Information Management System (ASIMS)
- Agile Core Services - Data Access Layer (ACS-DAL)
- Composite Health Care System (CHCS)
- Individual Longitudinal Exposure Record (ILER)
- Theater Medical Data Store (TMDS)
- Patient Discovery Web Service (PDWS)
- Health Artifact and Image Repository (HAIMS)
- Health Information Archives (HIA)
- Joint Legacy Viewer (JLV)
- TRICARE Online (TOL)
- Service Treatment Record (STR) Processing Operations Reports Tracking Solution (SPORTS)
- Defense Enrollment Eligibility Reporting System (DEERS)
- Uniformed Services (Army, Air Force, Navy, Marines)
- Veterans Affairs (VA)
- Department of Defense Healthcare Management System Modernization (DHMSM)
- Defense Information Systems Agency (DISA)
- Social Security Administration (SSA)
- Ward Engineering Support Services (WESSGRP)
- Legacy Data Consolidation Services (LDCS)
- Pharmacy Data Transaction Services (PDTS)
- VA Integrated Systems and Technology Architecture (VistA) Interface Engine (IE)
- VA Clinical Health and Data Repository (CHDR)

Existing DoD Information Databases include

- Clinical Data Repository (CDR)

Other Federal Information Systems:

- Federal Health Information Exchange (FHIE)
- Data Access Service (DAS)
- Legacy Viewer Service (LVS)
- Armed Forces Health Longitudinal Technology Application (AHLTA)

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

E-mail
 In-Person Contact
 Fax
 Information Sharing - System to System
 Other (If Other, enter the information in the box below)

Official Form (Enter Form Number(s) in the box below)
 Paper
 Telephone Interview
 Website/E-Form

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 referenced by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

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://dpcl.dod.mil/>
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

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.

GRS 3.1, item 012 (DAA-GRS-2013-0005-0008)

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

[Redacted]

(3) Retention Instructions.

FILE NUMBER: 1601-11

DISPOSITION: Temporary. Cut off and destroy when related master file or database has been deleted.

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.

Public Law 104-191, Health Insurance Portability and Accountability Act of 1996; 10 U.S.C., Chapter 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. 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.

The information collected in this system is for the diagnosis and treatment of medical disorders and is considered a public information collection in accordance with DoDM 8910.01, V2, Encl 3, paragraph 8b(5).