

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:

Defense Medical Logistics - Enterprise Solution (DML-ES) - Core (DML-ES - Core)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

08/22/23

Program Executive Office (PEO) Medical Systems (J-6)

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.

Defense Medical Logistics - Enterprise Solution (DML-ES) - Core provides a fully integrated automated information system that supports medical logistics functionality including medical supply, equipment maintenance, facility management, and assemblage management. Medical Logistics (MEDLOG) Information Technology (IT) solutions directly support the Defense Health Agency (DHA) and Information Operations - Health IT missions through IT solutions that integrate readiness and health to deliver: increased readiness, better health, better care, and lower cost by implementing, managing and sustaining integrated and protected information in order to ensure the right information is accessible to the right customers at the right time and in the right way. Users of DML-ES - Core include military and Veterans Affairs (VA) medical logicians; clinical staff working in military and VA treatment facilities; combat readiness planners; trainers at Services and VA school houses to include direct contractors and government staff.

The categories of individuals the personal information is collected or obtained from electronic systems include: active duty, reservist, National Guard personnel and retired military of both DoD and VA Military Treatment Facilities (MTFs). Users primarily access DML-ES - Core through the use of Common Access Card (CAC) and Personal Identity Verification (PIV); these access credentials are stored using PIV/CAC, Single Sign On, user ID and password.

DML-ES - Core collects demographic data such as contact information, personal identifier, geographic, and work force information to generate user accounts for system access, identification of user processed transactions, organizational alignment and record the loan of DoD property. The PII data is retained until the user no longer requires access/business need which is validated annually and the Government property is still considered on loan. There is no defined time frame for these business processes as it is based on the need. The PII data are shared with DoD and Federal systems of Procurement Integrated Enterprise Environment (PIEE), Wide Area Work Flow (WAWF) for confirmation of product receipt and to facilitate payment from the respective Service/Agency Financial systems and to inform VA systems of an expenditure of products.

DML-ES - Core receives and collects non-PII data to include: Medical, surgical, dental, equipment and pharmaceutical product information and product attributes; equipment maintenance actions, history and maintenance plans; building and facilities information and attributes; authorized stock and inventory balances; organizational information; and fund control points.

DML-ES Core is owned/managed by the MEDLOG IT Program Management Office (MEDLOG IT PMO)/Solution Delivery Division (SDD)/Program Executive Office (PEO) Medical Systems (J-6)/DHA.

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)

DML-ES Core collects PII for authentication and administrative use. The intended use of PII collected by DML-ES Core is to support system access authorization, audit and transaction execution history; support product receipt and inspection for financial payment and to

positively account for government property that is issued to an authorized direct contractor, beneficiary (retired or service-connected disability veteran) and government staff.

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 can object to the collection of their PII in writing, by declining to provide a completed DD2875 (System Authorization Access Request) or hand receipt for equipment issuance. However, if an individual chooses to object to the collection of their PII, they will not be authorized to access DML-ES Core or receive government issued property.

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 have the opportunity to consent to specific uses of their PII in writing, by declining to provide a completed DD2875 (System Authorization Access Request) or hand receipt for equipment issuance. However, if an individual chooses to withhold consent for specific uses of their PII, they will not be authorized to access DML-ES Core or receive government issued property.

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

DD Form 2875 (System Authorization Access Request form), Privacy Act Statement. Authority: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

Principal Purpose: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information.

NOTE: Records may be maintained in both electronic and/or paper form.

Routines Uses: None.

Disclosure: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

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)

- | | | |
|---|----------|--|
| <input checked="" type="checkbox"/> Within the DoD Component | Specify. | DHA MTFs |
| <input checked="" type="checkbox"/> Other DoD Components (i.e. Army, Navy, Air Force) | Specify. | Defense Logistics Agency (DLA) Information Operations (J-6); Departments of the Army, Navy, and Air Force. |
| <input checked="" type="checkbox"/> Other Federal Agencies (i.e. Veteran's Affairs, Energy, State) | Specify. | Department of Veterans Affairs (VA) |
| 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. | |
| 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)

- | | |
|---|--------------------|
| <input checked="" type="checkbox"/> Individuals | Databases |
| <input checked="" type="checkbox"/> Existing DoD Information Systems | Commercial Systems |
| <input checked="" type="checkbox"/> Other Federal Information Systems | |

Existing DoD Information Systems: Defense Enrollment Eligibility Reporting System (DEERS).

Other Federal Information Systems: VA Electronic Health Record (EHR) provides internal control numbers (ICNs); VA information system responsible for PIV certificate authentication.

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

- | | |
|---|---|
| <input type="checkbox"/> E-mail | <input checked="" type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input checked="" type="checkbox"/> In-Person Contact | Paper |
| <input type="checkbox"/> Fax | Telephone Interview |

Information Sharing - System to System

Website/E-Form

Other (If Other, enter the information in the box below)

Official Form: DD2875 (System Authorization Access Request).

Information Sharing – System to System: DEERS; VA EHR; VA information system responsible for PIV certificate authentication.

In-Person Contact: DD Form 1150, Request for Issue/Transfer/Turn- In, filled out by individuals requesting government property.

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 EDHA 28

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.

l. 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. NI-330-11-002, Item 1

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

(3) Retention Instructions.

FILE NUMBER: 911-12

FILE TITLE: Defense Medical Logistics Support System (DMLSS) Medical Logistics Master Files

DISPOSITION: Temporary. Cut off annually. Destroy 3 years after cutoff.

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.

DoDI 5 U.S. Code § 552a (Pub.L. 93-579, Privacy Act of 1974); 10 U.S. Code § 4601 - Electronic submission and processing of claims for contract payments; 10 U.S. Code § 1097(a) and § 1097(b), TRICARE Prime and TRICARE Program; 18 U.S. Code § 1030 (Pub.L. 99-474, Computer Fraud and Abuse Act of 1986); 5 U.S. Code § 301 - Departmental regulations; 44 U.S. Code § 3541 (Pub.L. 107-347, Federal Information Security Management Act of 2002); E.O. 10450 (Security requirements for Government employment); 32 CFR § 199.17 - TRICARE Program; Defense Federal Acquisition Regulation Supplement (DFARS) Procedures, Guidance, and Instructions (PGI) 232.70 and 252.232-7003; DoD Instruction 5000.75, Business Systems Requirements and Acquisition; DoD Instruction 5400.16, Department of Defense Privacy Impact Assessment; DoD Instruction 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property; E.O. 9397 (SSN), as amended; and Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

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.

DML-ES Core does not collect new PII information from members of the public. DML-ES Core collects information from Members of the Armed Forces and Veteran personnel in order to track equipment request approvals and coordinations, medical logistics issued equipment and accountability. Public collection, such as from spouses and dependents of members of the Armed Forces and DoD-affiliated personnel, are not collected.