

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:

My Military Health - Help Desk (MMH-HD)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

07/22/2025

DOD Healthcare Management System Modernization (DHMSM) / PEO Defense Healthcare Management Systems (DHMS)

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 My Military Health - Help Desk (MMH-HD) is an IT service desk application and self-service portal used by Leidos Partnership for Defense Health (LPDH) to track technical support requests from beneficiaries/patients, providers, and Military Treatment Facility (MTF) staff for the MyMilHealth applications. Additionally the MMH-HD is used to facilitate appointment notification and reminders to patients for scheduled virtual visits appointment. The MMH-HD application is built on the HealthForce Nexus (HFN) Salesforce Platform. This application supports Defense Health Agency (DHA) markets, and Outside of the Continental United States (OCONUS) sites.

Personal Identifiable Information (PII) may include numerous types of PII including employee and beneficiary contact information, military information, demographic information, Social Security Number (SSN), and Protected Health Information (PHI). PII processed on some system components, applications, and documents utilize specific administrative, physical, and technical security controls to protect PII confidentiality which may be addressed in separate Privacy Impact Assessments (PIA)s available at: <https://dodcio.defense.gov/In-the-News/Privacy-Impact-Assessments/>.

MMH-HD is owned by the Defense Healthcare Management System Modernization (DHMSM) Project Management Office (PMO), managed by the LPDH contract team, and hosted by DHA on the HFN platform residing within Salesforce GovCloud+.

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 to troubleshoot issues with My Military Health applications, contacting beneficiaries, and used for mission-related and administrative purposes. It is also collected to facilitate appointment notification and reminders to patients for scheduled virtual visits appointment.

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.

Contacting the help desk is optional for support and the act of contacting will provide their phone number and/or email. Data for the appointment notifications is controlled and sent from Military Health System GENESIS (MHS GENESIS).

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.

Contacting the help desk is optional for support and the act of contacting will provide their phone number and/or email. Data for the

appointment notifications is controlled and sent from Military Health System GENESIS.

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

The My Military Health Self-Service Portal users will be prompted with a warning that you are accessing a USG IS and consent to monitor when logging in with iAS.

Nothing is shared with an individual who contacts the MMH Help Desk via a phone call requesting support. Once the ticket is entered and if they share their email they will get an email confirmation of creation of their ticket. Emails to the MMH Help Desk will also get the same confirmation of ticket creation. DoD Banner Warning and consent to monitoring verbiage below:

Warning Notice and Consent to Monitor

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

At any time, the USG may inspect and seize data stored on this IS.

Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

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. | <input type="text" value="Components participating in DHMSM Program."/> |
| <input type="checkbox"/> Other DoD Components (i.e. Army, Navy, Air Force) | Specify. | <input type="text"/> |
| <input type="checkbox"/> Other Federal Agencies (i.e. Veteran's Affairs, Energy, State) | Specify. | <input type="text"/> |
| <input type="checkbox"/> State and Local Agencies | Specify. | <input type="text"/> |
| <input checked="" type="checkbox"/> 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. | <input type="text" value="The Leidos Partnership for Defense Health (LPDH)"/> |
| <input type="checkbox"/> Other (e.g., commercial providers, colleges). | Specify. | <input type="text"/> |

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

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

iAS unique ID mapped to the EDIPN (DoD ID Number) of the user.

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 checked="" type="checkbox"/> Telephone Interview |
| <input type="checkbox"/> Information Sharing - System to System | <input checked="" type="checkbox"/> Website/E-Form |
| <input type="checkbox"/> Other (If Other, enter the information in the box below) | |

We keep records of the individuals who contact the Help Desk in the form of person accounts and the cases that are created for them. The person accounts contain rolodex PII including the DOD ID. The case records are linked to the accounts and include details about the issue

they are reporting including the associated MTF location related to the issue. All cases will have an account record associated to them. Additionally scheduled virtual visits appointment data is stored to facilitate the sending of appointment notifications and reminders.

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.

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.

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

(3) Retention Instructions.

FILE NUMBER: 1606-10

FILE TITLE: Technical and Administrative Help Desk Operational Records

DISPOSITION: Temporary. Cut off after record is resolved or when no longer needed, whichever is appropriate. Destroy 1 year 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.

5 USC 301, Departmental Regulations; 10 USC 136, Under Secretary for Personnel and Readiness; 10 USC Chapter 55, Medical and Dental Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); Public Law 104-191, Health Insurance Portability and Accountability Act of 1996; DoD Manual 6025.18, Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs; 42 USC 290dd-2, Confidentiality Of Records; 42 USC Ch. 117, Sections 11131-11152, Reporting of Information; 45 CFR 164, Security and Privacy; and EO 9397 (SSN).

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 not considered a public information collection in accordance with DoDM 8910.01, V2, Encl 3, paragraph 8b(5).