

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:

DHA Amazon Web Services

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

01/23/25

Infrastructure & Operations (I&O) Division

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.

DHA Amazon Web Services (AWS) provides a multi-tenant Government cloud service platform that offers functionality to support capacities such as Platform as a Service (PaaS), a cloud computing model that provides a complete development environment for building, running, and managing applications, and Infrastructure as a Service (IaaS), a cloud computing model that provides access to IT infrastructure on demand, on a pay-as-you-go basis. Software as a Service (SaaS) is also supported by AWS GovCloud IaaS/PaaS (L4) for customers managing their own exchange servers within AWS GovCloud IaaS/PaaS (L4). AWS GovCloud IaaS/PaaS (L4) provides cloud security at the software layer that meets the security, privacy, and compliance needs of its customers.

Each Program of Record (POR) has a published PIA covering personally identifiable information (PII) collected and must meet stringent protection requirements to operate in the Military Health Environment. In addition, the customer can add additional security such as file integrity monitoring and log file monitoring to comply with specific regulatory or business agreement requirements.

PII contained within DHA-AWS includes Electronic Data Interchange Personal Identifier (EDIPI), billing information, usernames, business address, and PHI collected and managed by the owning POR via their ATO boundary responsibilities.

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)

The purpose and the intended use of collected PII is specific to a system component and is addressed in the sub-system's PIA. DHA AWS provides CLOUD functionality to authorized PORs for mission-related and administrative uses.

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.

This system receives PII from a system-to-system interface and the opportunity to object is only available at the source system.

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 the specific uses of their PII is specific to the method used by the respective system component and is addressed in the respective sub-system's PIA.

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

DHA AWS does not collect PII directly from individuals; however, system components, applications, and electronic collections within the system might collect PII. Refer to the respective system component, application, or electronic collection PIA for additional information.

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) sub-components and Military Treatment Facilities (MTFs)

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

Specify. Active Duty Military personnel assigned to DHA from the Departments of the Army, Navy, and Air Force

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

Specify.

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. Various contractors supporting DHA provide system administration for DHA AWS and adhere to the required PII safeguards in their respective contracts per Defense Federal Acquisition Regulation (DFAR) Supplement, Subpart 224.1 (Protection of Individual Privacy). The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect Government data; ensuring the confidentiality, integrity, and availability of data including data breach reporting and response requirements. When authorized access to PII, the contractor shall complete annual PII training requirements and comply with privacy protections under the Privacy Act (Clause 52.224-1 and 52.224-2). The contractor shall safeguard PII from theft, loss, and compromise, and shall safeguard, transmit and dispose of PII per DHA and DoD policies. The contractor shall mark developed documentation containing PII accordingly. Misuse or unauthorized disclosure may result in both criminal and civil penalties. Unauthorized disclosure of PII through negligence or misconduct can lead to task order removal or task order termination depending on the severity of the disclosure. Upon discovery of a PII breach, the contractor shall immediately notify the Contracting Officer and contracting officer representative (COR).

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

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

E-mail

Official Form (Enter Form Number(s) in the box below)

In-Person Contact

Paper

Fax

Telephone Interview

Information Sharing - System to System

Website/E-Form

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

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://dpclid.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.

The DHA AWS system is not a system of records.

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.

The LAN/Enclave itself does not have a NARA approved, pending, or GRS authority and retention instructions applied as a whole. Refer to NARA approved, pending, or GRS authority and retention instruction specific to the systems, applications, electronic collections, file servers, and share drives contained within the LAN/Enclave

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.

DoD Instruction 8500.01, Cybersecurity, 14 Mar 2014; DoD Joint Information Environment (JIE) Cyber Security Reference Architecture (CS RA) v 4.0 April 15, 2016; Computer Network Defense (CND) Service Provider Program via DoD Instruction 8530.01, March 7, 2016; DoD Instruction O-8530.2: Support to Computer Network Defense (CND), March 9, 2001.

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 conditions and not considered a public information collection per DoDM 8910.01, Volume 2, Enclosure 3, paragraph 8b(5); system does not collect information from members of the public.