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:

Zero Trust Architecture Framework Environment 2.0 (ZAFE)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

08/04/2026

Deputy Assistant Director Information Operations / PEO MS / CIO - J6/Combat System Agency Integration

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.

(1) Purpose and type of information technology: ZAFE is a zero-trust operational environment engineered by the DHA to deliver secure, resilient, and expeditionary digital capabilities for military medical and mission command operations. Built to thrive in contested, degraded, or remote environments. ZAFE represents a shift from traditional perimeter-based security to a model that assumes no implicit trust, protecting every user, device, and data transaction regardless of location.
At its core, ZAFE functions as a secure edge computing and virtualization platform enabling medical and mission critical digital services to operate autonomously while disconnected from enterprise networks. Hosted applications which support store-and-forward, get synchronized seamlessly when connectivity is restored. This dual mode capability allows these shaped field elements to maintain operational independence without sacrificing cyber security continuity or interoperability.
ZAFE also functions as a data diode between two different classifications of networks.

(2) General overview of the modules, subsystems, and their functions:

The Stationary Command and Control Node, referenced as the Headquarters ZAFE is always on and always available providing centralized storage, synchronization, auditing, and zero-trust orchestration. This end point receives data uploads from the Field portable ZAFE nodes, referenced as Remote ZAFE, once connectivity is restored. Remote ZAFE can be at Role 2 Clinical or Role 3 Military Treatment Facilities (MTFs) and connects to the enclave network via encrypted VPN tunnels. The Remote ZAFE can also share data with other remote ZAFEs through the Onclave Trusted Platform suite of software products (COTS).

In this scenario, the applications hosted on the ZAFE VM on the remote ZAFE uploads its data to the Headquarter ZAFE upon establishing a Wide-Area Network (WAN) connection. The WAN connection to the internet can be Ethernet, WiFi, Long-term Evolution (LTE), 5G, Satellite Communications (SATCOM), NIPRnet or SIPRnet.

Each node of ZAFE includes one or more physical server cards running Windows Server and various Hyper-V virtual machines (VM) which comprise the system. Other VMs include firewalls, Onclave TrustedPlatform and sub-components.

(3) Categories of individuals about whom the PII is collected for the system/electronic collection includes Federal employees (Military members of the Armed Forces, DoD civilian employees, etc.).

(4) Types (categories) of personal information collected: Name, DoD Identity Number, date of birth, employment information, official duty address/telephone number, and work address type information for active directory used to authenticate and grant account permissions.

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)*

User data is collected to support identification, authentication and authorization.

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.

In accordance with the Privacy Act of 1974, submission of information is voluntary. If an individual chooses not to provide their information, no penalty may be imposed, but absence of the requested information may result in administrative delays.

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.

In accordance with the Privacy Act of 1974, submission of information is voluntary. If an individual chooses not to provide their information, no penalty may be imposed, but absence of the requested information may result in administrative delays.

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: Public Law 99-474, the Computer Fraud and Abuse Act
PRINCIPAL PURPOSE(S): 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
ROUTINE USE(S): 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)*

☒ Within the DoD Component	Specify.	Authentication to applications residing within the ZAFE.
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Service owned applications residing within the ZAFE environment
☐ 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.	
☐ 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

The data contained in ZAFE is kept within the clinical applications that hold an ATO.

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)*

DD2875

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 DoD-0015

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

This system does not maintain records where the information is retrieved by the individual's name number or unique identifier.

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.

Mission Schedules:
- GRS 5.2, item 020 (DAA-GRS-2022-0009-0002)

Other Schedules:
- System Access Records: GRS 3.2, item 030 (DAA-GRS-2013-0006-0003),
- Data Administration and Documentation: GRS 3.1, item 051 (DAA-GRS-2013-0005-0003)

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

(3) Retention Instructions.

Mission Schedules:
FILE NUMBER: 103-14
FILE TITLE: Intermediary Records
DISPOSITION: Temporary. Cut off and destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later.
RM NOTE: Exported patient record information is maintained in the appropriate electronic health record system i.e. MHS Genesis.

Other Schedules:
FILE NUMBER: 1601-02
FILE TITLE: System Access Records - Systems not requiring Special Accountability for Access
DISPOSITION: Temporary. Cut off and destroy when business use ceases.

FILE NUMBER: 1601-12
FILE TITLE: Data Administration and Documentation - Temporary Systems
DISPOSITION: Temporary. Cut off after the project/activity/transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system. Destroy 5 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 statue 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.

AUTHORITY: 10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); DoDI 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFs); 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.

N/A: Component internal information collections that do not collect information from members of the public.