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 Enterprise (ZAFE)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

12/19/24

Deputy Assistant Director Information Operations / J-6 (DAD IO/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
- [x] 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.)*

- [x] 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: Zero-Trust Architecture Framework Enterprise (ZAFE) is a locally developed system that incorporates both COTS and Open Source Software (OSS) to create a secure, portable, Zero Trust Unified Theater Server Platform (UTSP) with an OSS version of Armed Forces Health Longitudinal Technology Application (AHLTA)-Theater (AHLTA-T), hereafter referred to as OpenAHLTA, a point-of-care clinical documentation and management application, while providing National Security Level protection that satisfies U.S. Executive Order 14028 for Zero Trust Architectures.

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

Onclave TrustedPlatform Components: Onclave TrustedOrchestrator is a single integrated interface that builds secure enclaves. It provides a dynamic deployment of secure virtual segmented networks over existing infrastructure. Onclave TrustedBroker is used to create trusted and secure communications with TrustedEdges. It has its own root of trust cypher key generator for establishing cryptographically encrypted layer 2 secure tunnels between Onclave TrustedBrokers and Onclave TrustedEdges. Onclave TrustedEdge is a device that forms the basis of a cryptographically layer 2 secure enclave using AES 256 (GCM) connected to an Onclave TrustedBroker. TrustedEdge initiates the layer 2 session tunnel with a TrustedBroker based on both devices having a bi-lateral trust. Onclave TrustedBlockchain is a private multi-segment and multi-path blockchain based on Onclave’s Dynamic Cipher Key Management (DCKM) patent design. Manages identities, trust, and state of Onclave TrustedOrchestrator, TrustedEdges, and TrustedBroker using GUIDs to enforce Identity Management.

Xiid.IM - AbsoluteZero Trust Platform for Identity Management and Data Access

OpenAHLTA is an OSS version of AHLTA-Theater (AHLTA-T), a point-of-care clinical documentation and management application that developed and is sustained by the Defense Health Information Management System (DHMS) and serves as the military’s electronic health record for service members in theater only. AHLTA-Theater maintains a comprehensive, lifelong, computer-based patient record for every soldier, sailor, airman, marine, and beneficiary entitled to Department of Defense military health care while they are in the theater of operations, such as Afghanistan and on ships worldwide. ZAFE does not store records indefinitely. Records are wiped after in theater use and after transmitting to the Master Cluster Management System (MCMS). OpenAHLTA provides instant access to a continuous and coherent chronology of the health care history of each patient and enables the rapid access and transfer of relevant patient information for regional and remote treatment of injuries and illnesses. Medical personnel use the solution to record patient clinical encounters and transmit those records to a central data repository making its data part of the patient's longitudinal electronic health record.

(3) Categories of individuals about whom the PII and PHI 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: OpenAHLTA collects a combination of PII (name, SSN) and PHI (Electronic Health Record (EHR) type information for use in the field/in Theater). The following types of personal information about individuals include: Name, Social Security Number (SSN), Race/Ethnicity, Birth Date, Address, Phone Number,Email, Religious Preference, Marital Status, Medical Information, Protected Health Information (PHI).

ZAFE is owned and operated by NIWC Pacific on behalf of DHA.
ZAFE is a NIWC Pacific prototype for DHA to be operated by medical personnel in Theater/field.

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 and PHI are collected to determine eligibility and administer healthcare delivery services, data matching of the individual with his/her EHRs, and to ensure accuracy when these reports are integrated in the medical records for that individual. User data is collected to support administration and clinical practice authorization and access. Clinical patient data is documented and stored in the OpenAHLTA patient files and is transmitted to the Master Cluster Management System (MCMS) when connected. The intended use of PII and PHI is Mission-related (patient healthcare) and administrative use. This data is used to provide continuity of patient care and patient care management.

e. Do individuals have the opportunity to object to the collection of their PII? [X] 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? [X] 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.

Consent to the specific uses of PII is obtained as necessary, in accordance with DoD 5400.11-R, DoD Privacy Program, C4.1.3. PHI is collected for permitted uses and disclosures as set forth by DoD 6025.18-R, DoD Health Information Privacy Regulation. Individuals are informed of these uses and are given the opportunity to restrict the use of their PHI based on the procedures in place at the local facility where the data is collected and maintained, in accordance with DoD 6025.18-R, C10.1. For uses other than Treatment, Payment and Healthcare Operations, individuals can authorize the use of their PHI by submitting DD Form 2870. For uses other than Treatment, Payment and Healthcare Operations, individuals can request restrictions on the use of the PHI by submitting DD Form 2871.
DD FORM 2930

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 [X] Not Applicable

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)*

[X] Within the DoD Component	Specify.	Clinical Data Repository (CDR), Theater Medical Data Store (TMDS), MHS GENESIS, Master Cluster Management System (MCMS)
[X] Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Air Force: Air Force Complete Immunization Tracking Application (AFCITA), Army: Medical Protection System (MEDPROS)
[X] Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Department of Veteran Affairs for the purpose of enabling DoD data retrieval from the Federal / Bi-Directional Health Information Exchange (FHIE/ BHIE) framework.
[ ] 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)*

- [x] Individuals
- [ ] Databases
- [ ] Existing DoD Information Systems
- [ ] Commercial Systems
- [ ] Other Federal Information Systems

The data contained in ZAFE is solely collected from and about Military Health System (MHS) beneficiaries for the purpose of providing health care. OpenAHLTA is similar to AHLTA-Theater (AHLTA-T); PII is collected from individuals at time of delivery of healthcare services.

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)*
- [x] 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
- [x] 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://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. Not Applicable

(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 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.

No/Not Applicable: ZAFE is still a prototype not a Program of Record (PoR) and, listed reason why OMB approval is not required IAW DoDM 8910.01, Volume 2, 2. APPLICABILITY
b. Does not apply to:
(1) Component internal information collections that do not collect information from members of the public.