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:

Compute and Storage Management Service (CSMS)

2. DOD COMPONENT NAME:

Defense Health Agency

Infrastructure & Operations (I&O) Division

3. PIA APPROVAL DATE:

05/15/23

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.)*

New DoD Information System	New Electronic Collection
X 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 Compute and Storage Management Service (CSMS) is a Defense Health Agency (DHA) system that provides computer processing and storage resources for hosted customers, which may include hosted servers, applications, databases, and file storage for Military Health System clinicians, pathologists, and other business users. Program Management Offices (PMOs) that host their application servers and databases on CSMS have their own published PIA for the potential protected health information/personally identifiable information (PHI/PII) that they collect and must meet stringent requirements to protect PII/PHI in order to operate in the Military Health Environment. DHA authorized database administrators (DBAs) are the only authorized users who may potentially have access to the databases that may contain PHI/PII outside of the Database Owners (who have accredited their database and any of its potential PHI/PII requirements), and this access is logged and would only be utilized at the request of the Database Owners for troubleshooting.

Another use case where CSMS as a system may have PHI or PII stored are the file servers and shares that are hosted on CSMS for end users' home drives, folder redirection, and departmental shares. It is possible that DHA end users (such as clinicians) may store PHI or PII on these file shares, though CSMS does not actively collect or disseminate that information, and by default, any data stored in user's home drives or folder redirection are permissioned for that user alone in accordance with the DoD security policies. Departmental shares, due to their less restrictive access controls, may contain PHI/PII only if allowed by established policy at Military Treatment Facility (MTF) sites. The responsibility for ensuring appropriate access controls for PHI/PII stored in Departmental shares solely resides with the DHA Administrators, who are responsible for their users' data and complying with subsequent Privacy Office and Health Insurance Portability and Accountability Act (HIPAA) requirements for PHI/PII. Other than the end users, DHA authorized Storage Administrators potentially have access to the user files and departmental files that may contain PHI/PII outside of the DHA end user, and this access would only be utilized for troubleshooting an issue with the user or potentially during incident response.

CSMS as a system comprised of the Application Virtual Hosting Environment and Local Core Infrastructure, and does not actively collect or disseminate PHI/PII information for use outside of the internal DHA organization. Information that could reside on the CSMS system depending on the end user's work-flow may include personal descriptors, ID numbers, ethnicity, health, financial, employment, or credit information for dependents, retirees and/or their dependents, active duty, contractors, foreign nationals, former spouses, reservist, and national guard personnel. CSMS only receives this information from a system-to-system interface with other systems that have an approved PIA on file.

The CSMS is owned and operated by 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)*

CSMS collects PII for mission-related and administrative uses. The intended use of the PII is to store for customer to utilize and access when necessary.

e. Do individuals have the opportunity to object to the collection of their PII? Yes x 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 only receives PII from a system-to-system interface and the opportunity to object is only available at the source system, which would be covered under a separate PIA for that source system.

f. Do individuals have the opportunity to consent to the specific uses of their PII? Yes x 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 do not have the opportunity to consent to the specific use of their PII because (system name) is not the initial point of collection.

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

The CSMS does not collect PII directly from individuals. Therefore, no Privacy Act Statement or Privacy Advisory is required.

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.	DHA Military Treatment Facilities
x	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Department of the Navy Department of the Army Department of the Air Force
	Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	
	State and Local Agencies	Specify.	

x	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 CSMS and adhere to the following safeguards for PII as required by their respective contracts in accordance with (Defense Federal Acquisition Regulation (DFAR) Supplement, Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoDD 5400.11, "DoD Privacy Program," May 8, 2007, and DoD 5400.11-R, "DoD Privacy Program," May 14, 2007): The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data. The Contractor shall also ensure the confidentiality, integrity, and availability of Government data in compliance with all applicable laws and regulations, including data breach reporting and response requirements. When a contractor, including any subcontractor, is authorized access to Personally Identifiable Information (PII), the contractor shall complete annual PII training requirements and comply with all privacy protections under the Privacy Act (Clause 52.224-1 and 52.224-2). The contractor shall safeguard PHI/PII from theft, loss, and compromise, and shall safeguard, transmit and dispose of PHI/PII in accordance with the latest DHA and DoD policies and the contractor's HIPAA Business Associate Agreement (BAA). The contractor shall mark all developed documentation containing PII information accordingly in either the header or footer of the document: "CUI – Privacy Sensitive. Any misuse or unauthorized disclosure may result in both criminal and civil penalties." Any unauthorized disclosure of privacy sensitive information 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). This list of contractors includes: Spinvi, Accelera Solutions, Core4ce, KSH, NSSPlus, BEAT, DXC.
	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	x	Databases
x	Existing DoD Information Systems		Commercial Systems
x	Other Federal Information Systems		

Armed Forces Health Longitudinal Technology Application (AHLTA),
Composite Health Care System (CHCS),
Essentris,
Coding and Compliance Editor (CCE),
IMPAX,
Fuji Synapse,
Special Needs Program Management Information System (SNPMIS),
Naval Medical Information System (NMIS),
Defense Medical Logistics Standard Support (DMLSS),
CareFX Context Management,
Vergence/Sentillion Context Management,
Veterans Information Systems and Technology Architecture (VistA),
Computerized Patient Record System (CPRS),

medical Joint Active Directory (mJAD),
Anatomic Pathology Lab Information System (APLIS), and
MHS GENESIS.

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
X	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.

The CSMS is not a system of records; however, system components, applications, and electronic collections that are used to collect individual information might require a System of Record Number (SORN). Refer to the specific system component, application, or electronic collection PIA for SORN information.

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. N/A

(3) Retention Instructions.

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 CSMS.

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.

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C., Chapter 55, Medical and Dental Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); 45 CFR 164, Security and Privacy; Department of Defense (DoD) Instruction 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFS); 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; 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 x 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.

CSMS as a system does not actively collect or disseminate PHI/PII information for use outside of the internal DHA organization. This system only receives PII from a system-to-system interface and the opportunity to object is only available at the source system, which would be covered under a separate PIA for that source system.