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:

Consolidated Information Center (CIC) Data Warehouse (a sub-system of BUMED Enclave)

2. DOD COMPONENT NAME:

Defense Health Agency

Bureau of Medicine and Surgery (Chief Data Office)

3. PIA APPROVAL DATE:

2/14/22

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

	From members of the general public		From Federal employees and/or Federal contractors
X	From both members of the general public and Federal employees and/or Federal contractors		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 Consolidated Information Center (CIC) Data Warehouse is used to facilitate the Bureau of Medicine and Surgery's analytical capabilities across Navy Medicine to improve speed of decision making. The CIC warehouse encompasses operational data store(s) that can serve enterprise decision support applications, inform gaps in data collection processes and systems, and facilitate knowledge transfer and management. The warehouse provides improved Business Intelligence, Analytics and Predictive Analytics capabilities that will be used by BUMED Headquarters and at the enterprise level. The types of projects enabled by CIC Data Warehouse include readiness dashboards, reports, ad-hoc data requests, data marts and identification of service members for readiness determinations. The CIC management serves as the primary overseer and access manager for data systems and tools utilized to support the Navy Medicine mission and equities. The data store(s) include both unstructured and structured electronic files. These files are sourced from multiple manpower, medical, logistics, human resource and financial systems. The CIC supports enterprise and Headquarters' Business Intelligence, Analytics, and Predictive Analytics capabilities. Types of projects enabled by CIC include readiness dashboards (e.g., medical, training, logistics and financial), reports, data support, ad-hoc data requests, data marts, and process improvements.

The CIC Data Warehouse collects Personally Identifiable Information (PII) consisting of contact information, military information, demographic information, Social Security Number (SSN), Protected Health Information (PHI), and medical information on Navy Medicine Readiness and Training Command personnel; other Military Health System employees, beneficiaries and contractors. The PII collected, maintained, analyzed and transmitted is used by government analytics personnel, program managers, system managers and other workforce members with a need to know. Data sourced from CIC may be shared within BUMED enterprise, Defense Health Agency, Chief of Naval Operations and Marine Corps.

Access to this information is controlled by the Chief Data Officer and Informatics Director. The system of records is supported by contractors who have appropriate clearance, federal acquisition regulation privacy, and cybersecurity requirements stipulated in their contracts. A Nondisclosure Agreement is signed before being given access to CIC. Workforce members who have access to the data are required to complete mandatory and supplemental privacy and cybersecurity training in accordance with Defense Health Agency (DHA), Department of the Navy (DON), and Department of Defense (DoD) policies.

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 PII is collected for a variety of uses, both mission-related and administrative. Primarily, the PII is required for workforce and patient identification, verification, and authentication for readiness tracking purposes, computer matching, and data analytics. Additionally, the PII could be used for data matching when interfacing and sharing data with external manpower, personnel and healthcare systems. Mission and Administrative related uses of the PII include personnel availability, unit readiness, and statistical analysis of health and fitness metrics. PII is not used for testing or research purposes.

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.

PII, including PHI maintained in the CIC data warehouse, is not collected directly from individuals. The CIC data is sourced from various DoD organizations, health, manpower, financial and logistics systems through data sharing agreements. Individuals have a right to object to the collection of their PII at the point of initial data collection, but not the data warehouse (repository).

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.

The CIC data warehouse is not the initial collection of PII and the opportunity to consent or withhold consent is not permissible. Consent to specific uses of PHI/PII is obtained as necessary from the authoritative systems or collection points sourcing the CIC electronic collection. All uses and disclosures of PII are in accordance with DoD 5400.11-R, DoD Privacy Program, C4.1.3. and DoDM 6025.18, Implementation of the HIPAA Privacy Rule in DoD Health Care Programs, and the system of record notices (SORNs) applicable to this electronic collection (See section 1.k. for listing of authoritative SORNs).

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

CICDW neither requests an individual to furnish PII to be included in either a (1) Privacy Act system of records nor (2) via a DoD website.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

x	Within the DoD Component	Specify.	Defense Health Agency (DHA)
x	Other DoD Components	Specify.	BUMED, Department of Navy (OPNAV & Marine Corps)
	Other Federal Agencies	Specify.	
	State and Local Agencies	Specify.	

			Contractors supporting CIC initiatives: Altarum Institute, Booz Allen Hamilton, Teledyne, Mantech, Center for Naval Analyses, Deloitte, Johns Hopkins University Applied Physics Lab The following language is contained in the above 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, and DoDM 6025.18, "Implementing HIPAA Privacy Rule in DoD Health Care Organizations," March 13, 2019.
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.	Personally Identifiable Information (PII) and Protected Health Information (PHI). 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, 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 also comply with federal laws relating to freedom of information and records management.
	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
x	Existing DoD Information Systems		Commercial Systems
	Other Federal Information Systems		

Military Health System (MHS) data sources:
Medical Data Repository (MDR)
MHS Mart (M2)
Armed Forces Health Longitudinal Technology Application (AHLTA)
Defense Medical Human Resources System internet (DMHRSi)
Joint Medical Asset Repository (JMAR)
Relias Education and Training Platform

Navy Systems:
Expeditionary Medicine Platform Augmentation Readiness Training System (EMPARTS)
Limited Duty Sailor and Marine Readiness Tracker System (LIMDU SMART)
DON Bureau of Personnel (BUPERS) Systems (FLTMPS)
Navy Manpower Planning and Budget Systems (NMPBS)

DoD Systems:
Defense Manpower Data Center (DMDC)
Defense Medical Logistics Standard Support (DMLSS)

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)*
	Face-to-Face Contact		Paper
	Fax		Telephone Interview
x	Information Sharing - System to System		Website/E-Form

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

Transfer of files via DoD Safe Data System Download and Data Sharing.

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.

x Yes No

If "Yes," enter SORN System Identifier EDHA-07; N06150-02

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.

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. Unscheduled

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

(3) Retention Instructions.

Unscheduled - Permanent. Treat system and/or records maintained in the system as permanent until a NARA approved schedule and disposition authority has been applied.

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.

Public Law 113-101, Digital Accountability and Transparency Act of 2006, as amended in 2014; Public Law 113-291, Federal Information Technology Acquisition Reform, 2015; 10 U.S.C. 2222, Defense Business Systems: Business Process Reengineering; Enterprise Architecture; Management; 10 U.S.C. 117, Readiness Reporting System; 10 U.S.C. 482, Readiness Reports; 31 U.S.C. 902, Authority and Functions of Agency Chief Financial Officers, as amended; 31 U.S.C. 3512(b), Executive Agency Accounting and Other Financial Management Reports and Plans; DoD Directive 7045.14, The Planning, Programming, Budgeting, and Execution (PPBE) Process; DoD Directive 7730.65, Department of Defense Readiness Reporting System; DoD Instruction 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense; DoD Instruction 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense; DoDM 6025.18, Implementing HIPAA Privacy Rule in DoD Health Care Organizations and E.O. 9397.

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.

CIC data warehouse is not a direct collection system of PII.