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:

Business Intelligence Common Services (BCS)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

12/21/23

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 Business Intelligence Common Services (BCS) serves as the Defense Health Agency (DHA) Solutions Delivery Division (SDD) Common Services environment for Data Analytics, Business Intelligence and Reporting requirements at the departmental and enterprise level. The BCS allows users to create standard, ad-hoc reports and post them in a secure Web environment to share with Military Health System (MHS) leaders. The BCS Security Model provides a common platform, with segregated access, based on the BCS Member Projects' registration workflows, row level security, and content organization. BCS provides a set of tools and interfaces for developers and end-users to create reports and analyze their data eliminating the need to master the underlying complexity of the data relationships. The SAP BI (Business Intelligence) Central Management Console (CMC) provides an administrator/developer interface for developing a security model (i.e., groups/folders/universe rights, etc.) and provides centralized administrator utilities which allow administrators to prepare and monitor statistics and activity within BCS. BCS offers availability of the SAP BI Launchpad, which provides robust ad-hoc reporting and desktop exporting.

BCS provides reporting and analytical services to the user communities are as follows:

- Defense Medical Human Resource System–internet (DMHRSi) Data Repository (DDR)
- Defense Occupational and Environmental Health Readiness System-Hearing Conservation (DOEHRS-HC)
- Defense Occupational and Environmental Health Readiness System – Industrial Hygiene (DOEHRS-IH)
- Expense Assignment System (EAS)
- Electronic Research Protocol Management System (EIRB)
- Health Artifact and Image Management Solution (HAIMS)
- Identity Authentication Services (iAS)
- Joint Medical Asset Repository (JMAR)
- Longitudinal Exposure Record (ILER)
- Military Health System (MHS) Management Analysis and Reporting Tool (MART) (M2)
- Pharmacy Operations (Pharmacy Ops)
- Patient Encounter Processing and Reporting (PEPR)
- Special Needs Program Management Information System (SNPMIS)
- Service Treatment Record (STR) Processing Operations Reports Tracking Solution (SPORTS)
- Spectacle Request Transmission System (SRTS)
- TRICARE Encounter Data (TED CRM) Information Systems

Members, former members, retirees, civilian employees (includes non-appropriated fund) and contractor employees of the DoD and all of the Uniformed Services; Presidential appointees of all Federal Government agencies; Medal of Honor recipients; U.S. Military Academy students; Lighthouse Service, DoD and Department of Veterans Affairs (DVA) beneficiaries (e.g. dependent family members, legal guardians and other protectors, prior military eligible for DVA benefits, Non-DoD Beneficiary and DoD Beneficiary, a person who receives benefits from the DoD based on prior association, condition or authorization, an example is a former spouse; Former member (Reserve service, discharged from Ready Reserve or Selective Reserve following notification of retirement eligibility); non-Federal agency civilian associates and other individuals granted DoD privileges, benefits, or physical or logical access to military installations (e.g., American Red Cross paid employees, United Service Organization (USO), Intergovernmental Personnel Act Employees (IPA), Boy and Girl Scout Professionals, non-DoD contract employees); members of the public treated for a medical emergency in a DoD or joint DoD/DVA medical facility; Non-DoD Civilian employee; and individuals requiring a Common Access Card to access DoD IT applications (i.e., Department of Homeland Security employees, state National Guard Employees, and Affiliated Volunteers); Civilian Retirees; DoD OCONUS Hires; Foreign Army; Foreign Navy; Foreign Marine Corps; Foreign Air Force; and Foreign Coast Guard.

The types of personally identifiable information (PII) shared between the systems are personal identifiers, demographic information, personal contact information, military information, medical information, disability information, education information, and other to include spouse information, child information, family member prefix (FMP), sponsor SSN, child's school address, other child care locations and provider's name and title that evaluate and provide intervention; clinics and medical summaries; individual educational program plans; Educational and Developmental Intervention Services (EDIS) process and activities data include referral, evaluation, eligibility, and service plans.

BCS administrators maintain the system, developers design/develop universes and reports available for end users to use, and end users refresh reports developed by developers or develop their own ad hoc reports.

BCS users may generate reports that include PII such as personal identifiers and demographic information.

BCS is owned and managed by DHA SDD.

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 obtained through BCS is collected for mission-related and administrative purposes. BCS is used as a conduit for analytic and reporting purposes for users who are reporting from applications as DMHRSi DDR, DOEHRS-HC, DOEHRS-IH, EAS, EIRB, HAIMS, iAS, M2, Pharmacy Ops, PEPR, SNPMIS, SPORTS, and TED CRM Information Systems.

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.

Individuals do not have the opportunity to object to the collection of their PII because BCS is not the initial point of collection.

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.

Individuals do not have the opportunity to consent to the specific uses of their PII because BCS 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 ☒ Not Applicable

BCS does not collect PII directly from individuals. Therefore, no Privacy Act Statement or 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)*

☒	Within the DoD Component	Specify.	MHS Applications that subscribe to BCS through iAS Authentication.
	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	
	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

[✓ Existing DoD Information Systems]

Other Federal Information Systems

Databases

[✓ Commercial Systems]

DMHRSi DDR, DOEHRS-HC, DOEHRS-IH, EAS, EIRB, HAIMS, iAS, M2, Pharmacy Ops, PEPR, SNPMIS, SPORTS, and TED CRM Information Systems.

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

E-mail

In-Person Contact

Fax

[✓ Information Sharing - System to System]

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

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

Paper

Telephone Interview

Website/E-Form

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 EDHA 07

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. GRS 5.2, item 020 (DAA-GRS-2017-0003-0002)

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

(3) Retention Instructions.

FILE NUMBER: 103-14
DISPOSITION: Temporary. Delete no more than 7 years from the date last modified. (See DoD DTM 22-001 on default disposition policies and OSD Records Manager guidance which file number to associate).

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; Federal Information Security Management Act of 2002 (44 U.S.C. 3554); E-Government Act of 2002 (Pub. L. 107-347, Sec. 203); Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et al.) and Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504 note); Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; 42 U.S.C. Chapter 117, Sections 11131-11152, Reporting of Information; DoD Instruction 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.

The information collected in this system is for the diagnosis and treatment of medical disorders and does not collect PII directly from individuals. It is not the initial point of collection for any PII and is not considered a public information collection IAW DoDM 8910.01, V2, Encl 3, paragraph 8b(5).