PRIVACY IMPACT ASSESSMENT (PIA)

For the

Clinical Enterprise Intelligence Program (CEIP)
Defense Health Agency (DHA)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	**New DoD Information System**	☐	**New Electronic Collection**
☒	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒	**Yes, DITPR**	Enter DITPR System Identification Number	16919
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☐	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☒ **Yes** ☐ **No**

If "Yes," enter UPI UII: 007-000100123

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier EDHA 07

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

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.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The goal of the Clinical Enterprise Intelligence Program (CEIP) is to advance patient-centered healthcare delivery through integration of informatics and thus transforming our enterprise to a rapid learning organization. CEIP is a collection of systems and databases used to deliver enterprise clinical data. These capabilities are included in CEIP: Program Management; Data Warehousing; Application Portal; Infrastructure and Operations; Application Support; Business Intelligence; Analytics. Types of projects enabled by this platform include clinical dashboards, reports, data feeds, ad-hoc data requests, and data-mart. The systems are housed within the Space and Naval Warfare Systems Command (SPAWAR) enclave at Charleston Naval Shipyard, South Carolina. The servers contain and process military medical data for use in data analysis and patient care. They deliver information to aid decision makers both at the military treatment facility level and at the enterprise management level. This capability subsequently provides an enhanced level of care for the Department of Defense; as well as other authorized individuals seeking medical treatment and interaction within the Military Health System.

The types of personal information about individuals contained in these systems include personally identifiable information (PII) and protected health information (PHI). The category of individuals includes anyone seen for treatment in any military treatment facility to include all Department of Defense active duty military, dependents, retirees, and retirees dependents. There may also be rare instances of others included if, for example if they were treated for emergent care in a military treatment facility.

These systems are managed by the Defense Health Agency (DHA), Health Information Technology (HIT) Directorate, Information Delivery Division (IDD).

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The privacy risks associated with PII/PHI collected are the unauthorized or accidental release of data, which can lead to identity theft and fraud. Access to PII/PHI information is limited to users and Information Technology (IT) support personnel with a need and approval for access. The servers are physically kept in a secure area and are logically maintained behind a secure firewall. Backups are kept on a local server and stored in an alternate location. Information is protected using accounts with logon and passwords and/or Public Key Infrastructure (PKI) token cards.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Information is used by authorized Defense Health Agency personnel such as analysts and senior managers, system administrators, and other IT support personnel.

☒ **Other DoD Components.**

Specify. Access to information is also given to analysts and senior managers in the medical departments within the Departments of the Army, Navy, and Air Force.

☒ **Other Federal Agencies.**

Specify. Access to information is also granted to certain analysts and senior managers in the Department of Veterans Affairs.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. Numerous contractors tasked with analysis and/or support of the systems will also be granted access to the information in these systems.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

CEIP is not a source system, nor is it the initial point of collection for PII. CEIP is downstream from the initial entry point for PII. The opportunity to object is only available at the initial point of data collection. The responsibility for this belongs with the source systems.

j. 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.

CEIP is not a source system, nor is it the initial point of collection for PII. CEIP is downstream from the initial entry point for PII. The opportunity to object is only available at the initial point of data collection. The responsibility for this belongs with the source systems.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☒ **None**

Describe each applicable format.

CEIP is a system of records under the Privacy Act of 1974. However, because CEIP does not serve as the initial point of collection for any records it contains, no Privacy Act Statement is required.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.