PRIVACY IMPACT ASSESSMENT (PIA)

For the

Armed Forces Integrated Clinical Database (ICDB)
Defense Health Agency

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(CEIP)

☐ **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(CEIP)

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 EDHA07

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; 42 U.S.C Chapter 117, Subchapters II and III, Reporting of Information, Definitions and Report, 32 CFR 199, Civilian Health and Medical Program for 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.

ICDB is used by medical personnel at Medical Treatment Facilities (MTFs), and others within the MHS medical community, to access data captured by the Composite Health Care System (CHCS). At each site, the ICDB database stores approximately 85% of CHCS data elements. ICDB hardware and software have been deployed since 2001 and is currently in production at more than 100 Military Health System (MHS)/ CHCS host site locations world-wide (Army, Navy, and Air Force). ICDB processes the extracted data and correlates the information from each of the source databases using a standard set of patient, provider, and other identifiers. ICDB provides a standard clinical interface that allows viewing of a wide range of clinical information pertaining to a single patient or group of patients.

The ICDB Portal, also known as the CarePoint Healthcare Application Suite (CHAS), provides a single point of access to a multitude of applications in support of the MHS. Health care providers and managers are provided with access from a military network to applications at the local MTF level as well as enterprise level applications with access to the consolidated global data. ICDB consists of a web-based enterprise application portal, a Clinical Information Database and a group of enterprise, clinical and patient applications. ICDB is designed to complement other MHS information data systems and supports the following user groups:

- MHS health care providers who are required to deliver and track appropriate and timely clinical services on all enrolled members of the military health care community.
- Clinical and Management users who require the capability to retrieve, maintain, analyze, display, track, manage, and print timely, accurate and accountable clinical services data.

ICDB collects patient name, social security number, Defense Enrollment Eligibility Reporting System (DEERS) identification number, gender, race, and medical information from CHCS.

All of the applications listed below are part of the ICDB system:

- Appointments: The Appointments application is a role based list (“My Appts” or “Our Appts”) that provides the ability for Users to display and print all the Daily/Weekly/Monthly appointments scheduled in CHCS.

- Patient Summary and Details: Patient Summary view gives Providers and Nurses a comprehensive view of patient information gathered over time from the most commonly used modules of CHCS on one customizable screen coupled with the ability to drill down to over 5 years of patient clinical detail data.

- List Manager: List Manager provides the ability to display dynamic list of patients as well as the ability to build and maintain static lists of patients.

- Looking Glass: Provides users with a single integrated view of statistical data.

- Cross Service Visibility (CSV): CSV provides the ability for Nurses and Technicians to display all the Active Duty appointments scheduled for a selected Facility on a selected day.

- Peer Review Tracking (PRT): Provides the ability to conduct automated peer/chart reviews using standardized methodology on both in and outpatient records for either AHLTA or the paper record.

- Proactive Patient Management (PPM): Provides Healthcare Integrators (HCI)s and other clinical Users a manageable way to use data obtained from the MHSPHP.

- Dysplasia Patient Tracking (DPT): Provides the ability to quickly notify patients of Pap smear results as they become available in CHCS as well as track Dysplasia patients through all follow-up procedures.

- PCM Patient Referrals (PCMPR): Displays a list of all the referrals made for a provider's enrolled patients. From this list Users can drill down to the 'Referral Details' of each individual referral performed for a selected patient.

- Completed TELECONS: Displays a list of all the completed telephone consults for provider's enrolled patients. From this list Users can drill down to the details of each individual telephone consult performed for a selected patient.

- Referral Management System (RMS): Provides MTF users with the ability to electronically fax referrals in CHCS from the RMC to the MCSC.

- Referral Management System Tracking Reports (RMSTR): Provides MTF users with the ability to query on all referrals and in-house specialty care consults.

This system is owned and managed by the DHA, Health Information Technology Directorate, Information Delivery Division.

(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 the PII/PHI collected are the unauthorized release of data, which can lead to identity theft and fraud.

Access to PII/PHI information is limited to medical personnel with a need-to-know and the servers are kept in secure areas. Backups are either on a sever in the MTFs computer room or kept in a safe, if downloaded on tape. All information is protected using User ID and password or biometrics.

All production instances of ICDB are located behind firewalls on base or MTF networks. ICDB operates entirely within the boundaries of the firewalls, except for the boundary crossings described in the ICDB ports and protocols matrix.

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 DoD health care providers (such as MTF physicians, pharmacists, and nurses) and managers for the purpose of medical treatment. In addition the information may be used by personnel in billing and financial departments within the DHA for the purposes of billing, payment, and managing the business plan.

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify.

☐ **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.

ICDB is not the initial point of collection for PII. The individual will not have the opportunity to object to their collection for this system. The opportunity to object is only available at the initial point of data collection. This system is downstream from the initial point of data collection. The responsibility for this belongs with the source system.

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.

ICDB is not the initial point of collection for PII. The individual will not have the opportunity to object to their collection for this system. The opportunity to object is only available at the initial point of data collection. This system is downstream from the initial point of data collection. The responsibility for this belongs with the source system.

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.	ICDB does not collect PII directly from the patient, as it is not the source system. Privacy Act Statement and Privacy Advisory are the responsibility of the source system at initial point of collection.

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.