PRIVACY IMPACT ASSESSMENT (PIA)

For the

Department of Defense Consolidated Cancer Registry (CCR) System
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
- ☐ **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

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 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.

The purpose of this collection is to provide a database that consolidates all patient records found in the Automated Central Tumor Registry (ACTUR) system to better support DoD health care management programs and research. In ACTUR, patients undergoing cancer treatment at different facilities are seen as different patients. For example, a patient seen at three different military treatment facilities (MTFs) will have different ACTUR records at each MTF. In the CCR, these records are consolidated resulting in one record for the patient. This system obtains all its data from the Defense Enrollment Eligibility Reporting System (DEERS) before it is consolidated.

CCR receives personally identifiable information (PII) from ACTUR that includes medical information as well as name, Social Security Number (SSN), phone numbers, age, addresses, emails, medical record numbers, race, and date of birth are collected. PII is collected about DoD Service members (active or retired) and their dependents.

Joint Pathology Center (JPC) personnel will operate and provide oversight of the system. JPC is a component of DHA and is acting as a business associate of DHA as defined in the HIPAA Privacy Rule (45 CRF Parts 160 and 164, Subpart D) and DoD 6025.18-R, DoD Health Information Privacy Regulation. Because JPC is acting as a business associate of DHA in connection with maintaining and operating the CCR System to support DHA and Military Health System healthcare management programs, and to assure that uses and disclosures of CCR data for research and other purposes comply with the provisions of the HPAA Privacy Rule and DoD 6025.18-R, PII it receives from DEERS/ACTUR is classified as "protected health information" (PHI) as defined in the HIPAA Privacy Rules and DoD 6025.18-R. JPC subcontractors supporting the CCR System and having access to PHI held in CCR are deemed business associates of JPC.

(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 collection of PII are low. The security features of JPC provide a level of protection that meets or exceeds the minimal requirements of DoD Directive 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT). The concept of identification and authentication "layered protection" is used to keep unauthorized users out of the system. All personnel granted access must participate in a security training and awareness program. This program consists of both initial security training and annual refresher training. The CCR is maintained in the Walter Reed National Military Medical Center network, requires Common Access Card (CAC) access, and PII within the system is only available to properly authorized users under the oversight of the JPC.

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. For treatment, research, legal or regulatory purposes

☒ **Other DoD Components.**

Specify. Military Services as this is a DoD-wide collection for same purposes

☒ **Other Federal Agencies.**

Specify. U.S. Department of Veterans Affairs, Department of Health and Human

Services, National Institute of Health (NIH) as required by institutional review board (IRB)-approved research protocols.

☒ **State and Local Agencies.**

Specify. State Cancer Registries as required by Services Cancer Registry regulations

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

Specify. ICF Incorporated. Confidentiality / HIPAA. The Contractor Employee shall abide by AR 40-3 and AR 40-66 concerning the nature of limited privileged communication between patient and health care provider for security and personnel reliability programs. The Contractor EMPLOYEE shall abide by AR 40-66 concerning the confidentiality of patient records, as embodied in federal statutes including the Privacy Act of 1974 and the Drug and Alcohol Act, Public Law 92-129 and HIPAA. The Contractor EMPLOYEE shall direct all requests for medical information on patients to the Chief, Patient Administration Division. The Contractor EMPLOYEE shall not release any medical or personal information on a patient without first receiving written approval from the government. Government will provide the regulations upon request by the Contractor EMPLOYEE.

☐ **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.

The CCR is not the initial point of collection for PII. All data comes from ACTUR. Individuals have the opportunity to object in ACTUR.

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.

The CCR is not the initial point of collection for PII. All data comes from ACTUR. Individuals have the opportunity to consent in ACTUR.

A waiver is submitted to the Privacy Board for research purposes and no PII is shared with investigators without approval. The waiver satisfies the following criteria:

(a) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
1. An adequate plan to protect the identifiers from improper use and disclosure;
2. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
3. Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted.

(b) The research could not practicably be conducted without the waiver or alteration nor without access to and use of PHI.

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.

Although CCR may qualify as a system of records, it is not the initial point of collection for personally identifiable information (PII). CCR collects PII from other systems rather than directly from individuals. Accordingly, a Privacy Act Statement is not 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.