PRIVACY IMPACT ASSESSMENT (PIA)

For the

Composite Health Care System (CHCS)
TRICARE Management Activity (TMA)

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: 127
- ☐ **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: 007-000000435

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 DHA 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 C.F.R. 199.17 TRICARE Program; DoDI 6015.23, Delivery of Healthcare at Military Treatment Facilities; DoDI 6025.13, Medical Quality Assurance (MQA) and Clinical Quality Management in the Military Health System (MHS); 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.

CHCS is a fully integrated health care information system used in Department of Defense (DoD) Military Treatment Facilities (MTFs) and clinics. It is used to automate and integrate the functions performed by the hospital staff and to facilitate the delivery of health care and MTF administration. Data elements include beneficiary information collected and used to support the delivery of health care to TMA beneficiaries. In addition, user data is collected to support authentication, authority, and access to CHCS.

Personally identifiable information (PII) and protected health information (PHI) is collected to determine eligibility and administer health care delivery services. User data, which contains some PII and PHI, is collected to support administration and clinical practice authorization and access. Clinical patient data is documented and stored in the patient files in CHCS. Data is used for patient care management. Defense Enrollment Eligibility Reporting System (DEERS) is the source system for patient demographics, enrollment, and eligibility data.

The personal information collected in this system are as follows:
Name
Other names used
Social security number (SSN)
DEERS ID
Citizenship
Legal status
Gender
Race/Ethnicity
Birth date
Place of birth
Personal cell telephone number
Home telephone number
Mailing/Home address
Religious preference
Mother's maiden name
Mother's middle name
Spouse information
Marital status
Child information
Financial information
Medical information
Disability information
Employment information
Military record
Emergency contact

The information stored in this system consists of PII protected by the Privacy Act and PHI protected by Health Insurance Portability and Accountability Act (HIPAA). The individuals whose information is stored in this system include active duty military (all services + Coast Guard and Reserve), veterans, dependents, retirees and/or their dependents, active-duty, contractors, foreign nationals, former spouses, reservist, national guard personnel, and prisoners of war.

The system is located at Service Military Treatment Facility, Medical Centers and Hospitals: Uniformed Services Treatment Facilities. CHCS is accessed at multiple locations by users affiliated with Defense Health Information Management System (DHIMS) and by users at 105 MTFs.

The system does not host a Web site accessible by the public.

The point of contact for the system is:

Associate Director, EHR Sustainment and Deployment
5109 Leesburg Pike, Suite 701
Falls Church, VA 22041
(703) 681-6889

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

CHCS is susceptible to the same privacy risks inherent in any system collecting, using, and sharing PII/PHI. If this system is not properly protected then the PII/PHI contained therein could be accessed by unauthorized individuals through various methods such as data interception, unauthorized access, internal threats, and external threats.

CHCS data is encrypted in transit to protect against data interception. Unauthorized access and internal threats are mitigated by limiting the access to PII/PHI to trusted individuals only; these individuals have clearance and a "need to know" in order to access data. User and system authentication is addressed by verifying need to know and clearance. External threats are mitigated by following Defense Information System Agency (DISA) provided checklists as part of the CHCS Accreditation efforts under DoD Information Assurance Certification & Accreditation Program (DIACAP). This ensures that all necessary checks are followed to maintain the security of the CHCS system.

Therefore, all applicable security and privacy processes and regulations (e.g., DIACAP, HIPAA, etc.) required of a DoD system in operation have been defined and implemented, reducing risks to the maximum extent possible and to the point that any remaining risk has been accepted by the CHCS Designated Approving Authority (DAA). CHCS is currently accredited with a 3 year Authority to Operate (ATO).

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.

☒ **Other DoD Components.**

Specify. Army, Navy, Air Force

Army Blood Testing Service (ABTS), ADM/Business Objects Reporting System (ADM BOBJ), Agfa, AudioCARE System (ACS), Automatic Tablet Counter (ATC), Baker Cell 2000 (B2K (LPO)), Bidirectional Healthcare Information Exchange (BHIE), Centralized Credentials and Quality Assurance System – DHSS Messaging Gateway (CCQAS or RMG), CHCS Lab Interop (see DoD/VA CHCS, HML, Epilab, Labcorp, Quest) (Lab Interop, Lab Sharing), Comprehensive Ambulatory Professional Encounter Record (CAPER), Clinical Information System (CIS-Essentris), Come Anatomic Pathology System (CoPath), TriCare Consolidated mail Outpatient Pharmacy (TMOP), Consolidated Mail Outpatient Pharmacy (CMOP), Defense Blood Standard System (DBSS), Digital Imaging Network - Picture Archiving and Co (DIN-PACS (Agfa, Fuji, IBM, GE, Phillips & MedWeb)), Dictaphone Enterprise Express System (DEES), Embosser, Executive Information/ Decision Support (EI/DS), Enterprise Wide Scheduling and Registration (EWSR), Federal Healthcare Information Exchange (FHIE, GCPR), Fuji, Global Business Data Warehouse (GBDW), HIV Management Loader (HML), Information Exchange Platform (IXP), INTL Business Machine (IBM), Integrated Clinical Database (ICDB), Joint Patient Tracking Application (JPTA), KG Ambulatory Data System (KG ADS), Lab Data Sharing Initiative (LDSI) CHCS (LDSI CHCS), Lab Data Sharing Initiative (LDSI) DODHML (LDSI DODHML), Lab Data

Sharing Initiative (LDSI) LABCORP (LDSI LABCORP), Lab Data Sharing Initiative (LDSI) QUEST (LDSI QUEST), Lab Data Sharing Initiative (LDSI) VISTA (LDSI VISTA), Mammography Reporting System (MRS), McKesson Inpatient Robot - RX Interface (McKesson), Medical Records Retirement and Retrieval System (MRRRS), Medweb, National Enrollment Database (NED), Net Trials (NetTrials), Nutrition Management Information System (NMIS), Operating Room Management Application (ORMA), Pharmacy Data Transfer System (PDTS), Population Health Support Division (PHSD), Preventative Health Care Application (PHCA), Provider Graphical User Interface (P-GUI), Pyxis, Regional Breast Care Network System (RBCNS), Standard Ambulatory Data Report (SADR), Standard In-Patient Data Record (SIDR), Standard Insurance Table/Other Health Insurance (SIT/OHI), Site S Caché Shadowing, TNEXT PCM Enrollee NMIMC (TNEXT PCM), Translux Data Wall, Transportation Command (TRANSCOM) Regulating and Command and Control Evacuation System (TRAC2ES), TRICARE OnLine (TOL), United Services Prescription Database (USPD),Defense Finance and Accounting Service (DFAS), Electronic Prescribing (eRx).

Defense Enrollment Eligibility Reporting System (DEERS) is the source system for patient demographics, enrollment, and eligibility data.

To the U. S. Coast Guard (USCG) for USCG beneficiaries treated at DoD MTFs.

☒ **Other Federal Agencies.**

Specify.

To permit the disclosure of records to the Department of Health and Human Services (HHS) and its components for the purpose of conducting research and analytical projects, and to facilitate collaborative research activities between DoD and HHS.

To federal offices and agencies involved in the documentation and review of defense occupational and environmental exposure data, including the National Security Agency, the Army Corps of Engineers, National Guard, and the Defense Logistics Agency.

To the Congressional Budget Office for projecting costs and workloads associated with DoD medical benefits.

To the Department of Veterans Affairs (DVA) for the purpose of providing medical care to former service members and retirees, to determine the eligibility for or entitlement to benefits, to coordinate cost sharing activities, and to facilitate collaborative research activities between the DoD and DVA.

To the National Research Council, National Academy of Sciences, National Institutes of Health, Armed Forces Institute of Pathology, and similar institutions for authorized health research in the interest of the Federal Government and the public. When not essential for longitudinal studies, patient identification data shall be deleted from records used for research studies. Facilities/activities releasing such records shall maintain a list of all such research organizations and an accounting disclosure of records released thereto.

☒ **State and Local Agencies.**

Specify. To local and state government and agencies for compliance with local laws and regulations governing control of communicable diseases, preventive medicine and safety, child abuse, and other public health and welfare programs.

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

Specify. Data Exchange occurs between CHCS and individual Service readiness applications, contractor systems providing clinical results, personnel systems, workload management systems, Defense Manpower Data Center (DMDC), other developers and help desk support. For example, Lab Corp, Quest and EpiLab are contractors that perform patient specimen laboratory testing. CHCS sends electronic demographics and clinical orders, they send the lab results back to CHCS. When access to PII/PHI is required there is a supporting Data Use Agreement (DUA) in place (e.g. DMDC-Science Applications International Corporation (SAIC), SAIC-DHIMS, etc).

☐ **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.

Submission of information is voluntary. If an individual chooses not to provide PII/PHI information, no penalty may be imposed, but absence of the requested information may result in administrative delays

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

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.

Consent to the specific uses of PII is is obtained as necessary, in accordance with DoD 5400.11-R, DoD Privacy Program, C4.1.3. PHI is collected for permitted uses and disclosures as set forth in DoD 6025.18-R,

DoD Health Information Privacy Regulation. Individuals are informed of these uses and are given the opportunity to restrict the use of their PHI based on the procedures in place at the local facility where the data is collected and maintained, in accordance with DoD 6025.18-R, C10.1.

For uses other than treatment, payment and healthcare operations, individuals can authorize the use of their PHI by submitting DD Form 2870. For uses other than treatment, payment and healthcare operations, individuals can request restrictions on the use of the PHI by submitting DD Form 2871.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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.

AUTHORITY: 10 U.S.C. Chapter 55, Medical and Dental Care; 32 C.F.R. 199.17 TRICARE Program; DoDI 6015.23, Delivery of Healthcare at Military Treatment Facilities; DoDI 6025.13, Medical Quality Assurance and Clinical Quality Management in the Military Health System; and E.O. 9397 (SSN), as amended.

PURPOSE: To collect information from individuals necessary to determine eligibility, support authentication, and administer health care delivery services, to support administration and clinical practice authorization and access, and for patient care management.

ROUTINE USES: Information in your records may be disclosed to private physicians and Federal agencies, including the Department of Veterans Affairs, Health and Human Services, and Homeland Security in connection with your medical care; other government agencies to determine your eligibility for benefits and entitlements; and government and nongovernment third parties to recover the cost of healthcare provided to you by the Military Health System. Use and disclosure of your records outside of DoD may also occur in accordance with the DoD Blanket Route Uses published at http://dpclo.defense.gov/privacy/SORNs/blanket_routine_uses.html and as permitted by the Privacy Act of 1974, as amended (5 U.S.C. 552a(b)).

Any protected health information (PII) in your records may be used and disclosed generally as permitted by the HIPAA Privacy Rule (45 CFR Parts 160 and 164), as implemented within DoD.. Permitted uses and discloses of PHI include, but are not limited to, treatment, payment, and healthcare operations.

DISCLOSURE: Voluntary. If you choose not to provide your information, no penalty may be imposed, but absence of the requested information may result in administrative delays.

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.