PRIVACY IMPACT ASSESSMENT (PIA)

For the

Clinical Information System (CIS)/Essentris®
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 144

☐ **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: 007-000000379

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; DoD Instruction 6015.23, Delivery of Healthcare at military treatment facilities: Foreign Service Care; Third-Party Collection; Beneficiary Counseling and Assistance Coordinators (BCACs); 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.

Clinical Information System (CIS)/Essentris®, the Military Health System inpatient documentation solution, is a comprehensive clinical documentation system for use in acute care hospitals. CIS/Essentris® enables continuous and automated clinical documentation and bedside point-of-care data capture. All inpatient clinical documentation is created and stored in CIS/Essentris®, the Composite Health Care System (CHCS), and bedside instruments. Clinical data may be aggregated, trended, and analyzed to manage care for a single patient or for an entire patient population. CIS/Essentris® also provides waveform documentation, graphical trending on patient parameters, a reference library, patient education materials, and various reporting capabilities such as change of shift reports, task lists, and administrative reports.

CIS/Essentris® ensures that those records are accessible to providers throughout the remainder of the care continuum. Information from inpatient records captured in CIS/Essentris® will be accessible to other providers in the care continuum through the Bidirectional Health Information Exchange (BHIE) via the Department of Defense/Department of Veterans Affairs (DoD/VA) sharing data exchange framework. This level of interoperability will help ensure continuity of care for wounded warriors returning to the U.S. for additional care in DoD or VA facilities.

The data contained in CIS/Essentris® is collected solely from and about MHS beneficiaries for the purpose of providing requested health care. Personally identifiable information (PII) and protected health information (PHI) collected includes the following: name, Social Security Number (SSN), gender, date of birth, place of birth, telephone number (home and/or cell), mailing/home address, race/ethnicity, marital status, spouse information, child information, mother's middle and maiden name, medical information, employment information, citizenship, religious preference, and emergency contact. Additional information may be collected from dependents, retirees and their dependents, active duty, contractors, foreign nationals, former spouses, Reservists and National Guard personnel.

CIS/Essentris® is an unclassified commercial off the shelf (COTS) system supporting the delivery of inpatient, emergency department, and selected outpatient care at DoD military treatment facilities (MTFs). TMA has purchased licenses and is under contract to utilize this COTS product, owned by the vendor, CliniComp International. CIS/Essentris® has been successfully deployed at 59 critical care MTFs. TMA operates the system at all sites, with support from the vendor. TMA does not own the system.

System point of contact:
Inpatient Product Line Manager
5113 Leesburg Pike, Suite 701
Falls Church, VA 22041
(703) 681-7143

(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 personally identifiable information (PII)/protected health information (PHI) collected are due to sharing, using, and gathering PII/PHI. However, all applicable security and privacy processes and regulations have been defined and implemented, reducing risks and safeguarding privacy.

The MTFs computer facilities housing the CIS/Essentris® application and network communication servers have physical, technical, and administrative controls created in accordance with local policies such as office door locks, password-enabled screen savers, monitoring by facility staff, and application timeouts. The CIS/Essentris® technical controls, which prevent unauthorized individuals from logging onto the system, provide protection for unattended workstations.

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. Composite Health Care System (CHCS), Nutrition Management Information System (NMIS) - outbound inpatient food orders

☒ **Other DoD Components.**

Specify. Bidirectional Health Information Exchange (BHIE)

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify. Tier III support personnel at CliniComp International will have access to PII/PHI data but are not authorized to download any data without the site's permission. The contract contains the appropriate Business Associates Language as required.

☐ **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 PII is voluntary; however, if an individual refuses to provide needed 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 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.

(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.

A Privacy Act Statement is presented to individuals prior to system users entering any information into the CIS/Essentris® application and prior to their PII/PHI being collected.

AUTHORITY: 10 U.S.C. Chapter 55, Medical and Dental Care; DoD Instruction 6015.23, Delivery of Healthcare at Military Treatment Facilities: Foreign Service Care; Third-Party Collection; Beneficiary Counseling and Assistance Coordinators (BCACs); and E.O. 9397 (SSN), as amended.

PURPOSE: To obtain information from individuals necessary for continuous and automated clinical documentation and bedside point-of-care data capture, and to provide integrated functionality to military treatment facility staffs, facilitate the delivery of health care, and facilitate military treatment facilities administration. Information collected will be used to determine eligibility, administer health care delivery services, and provide for patient care management and reporting.

ROUTINE USES: Information collected may be used and disclosed generally as permitted under 45 Code of Federal Regulations (CFR) Parts 160 and 164, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, as implemented by DoD 6025.18-R, the DoD Health Information Privacy Regulation. In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the DoD “Blanket Routine Uses” under 5 U.S.C. 552a(b)(3) apply to this collection. Information from this system may be shared with the Departments of Health and Human Services, Homeland Security, and Veterans Affairs, the Congressional Budget Office, and other federal agencies; state and local governments and agencies for compliance with

laws governing communicable disease control, preventative medicine and safety, child abuse, and other public health matters; and private entities under contract with DoD for outpatient and other third party claims management purposes.

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.