



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Clinical Case Management (CCM)
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.**



**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; 45 C.F.R. Parts 160 and 164, Health Insurance Portability and Accountability Act, Privacy and Security Rules; DoDD 6040.37, Confidentiality of Medical Quality Assurance; and, E.O. 9397 (as amended, SSN).

**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 Case Management System (CCM) supports all three Services. It provides them with a documentation and tracking tool for Case Managers (CMs) managing the wounded, ill, and injured warriors, as they traverse through the federal health care system. The system will collect personal information from the active-duty member such as: name, gender, race, home address, unit assigned, telephone numbers, SSN, date of birth, and medical history.

The CCM application will support the clinical case management for the wounded, ill and injured (WII) patient community. The information infrastructure will leverage AHLTA and focus on supporting the health and medical needs of eligible DoD personnel by maximizing patient information processing functionality and outcome measurements.

The production of CCM will leverage foundation components of the Clinical Health Management System (CHMS) case management application that is currently used by case managers in the TRICARE South region. The CCM will support the entire case management workflow to include the collection of patient information, treatment planning based on Clinical Practice Guidelines, patient care monitoring, and case manager activity reporting.

The CCM application will provide a web-enabled user interface to support data collection, monitoring, and reporting activities of the Case Manager. The CCM system will be built on the foundation of the existing TRICARE Management Activity (TMA) architecture and appropriate CHMS case management components. The CCM application has been designated as a Congressional Line of Action (LOA) program. This places extreme criticality on the development and deployment of the application.

The CCM will interact with servers at the Department of Defense (DoD) enterprise level, including AHLTA, Composite Health Care System (CHCS), and the central repository Theater Medical Data System (TMDS). The CCM will be located at Defense Information Systems Agency (DISA) Montgomery, and client workstations at the Military Treatment Facilities (MTF)'s and clinic level.

Program Name = Defense Health Information Management System

POC Title = Project Lead

Telephone Number = 703-681-7150

Business Address = 5113 Leesburg Pike Suite 701, Falls Church, Virginia 22041

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

Misuse of data (including identity theft, blackmail and public embarrassment), unauthorized disclosure of data, and unauthorized modification or destruction of CCM sensitive data are risks associated with the Personally Identifiable Information (PII) and Protected Health Information (PHI) collected by this system. These risks are addressed by the use of smart cards used for validation and authentication required to access the system, Advanced Encryption Standards (AES), encryption of data at rest and in transit, and finally role-based security, which ensures that access to the information in the system is limited by job requirement and authorization to view the data.

Records are maintained in a secure, limited access, or monitored area. Physical entry by unauthorized persons is restricted by the use of locks, guards, or administrative procedures. Access to personal information is limited to those who require the records to perform their official duties. CCM users will be authenticated using Common Access Cards (CAC) and their access to data limited by their assigned roles within the CCM application. All personnel whose official duties require access to the information are trained in the proper safeguarding and use of the information.

**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.

**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.

Individual's PII/PHI is required to provide care and treatment needed by the individual. Additionally the information provided by the system is required for the CMs to successfully accomplish their mission. All submission of information is voluntary and initial consent occurs prior to the collection of information, however an individual's objection to the collection of PII/PHI would severely hinder the evaluation process.

(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.

When an individual is entered into the CCM system they are asked to acknowledge their participation in the CCM process which includes the sharing of information with authorized CCM system users. Individual's PII/PHI is collected for permitted uses and disclosures as set forth in DoD 6025.18-R, DoD Health Information Privacy Regulation.

(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 beginning the CCM process and prior to their PII/PHI being collected.