PRIVACY IMPACT ASSESSMENT (PIA)

For the

Coding and Compliance Editor (CCE)
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: 131
- ☐ **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: 007-000000137

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.

5 U.S.C 301, Departmental regulations; 10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); 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 Coding and Compliance Editor (CCE) system is a suite of commercial off-the-shelf (COTS) products that allows the Military Health System (MHS) to implement a solution focusing on an important series of coding, compliance, and data management objectives. The CCE product suite brings the MHS closer to a commercial coding and billing environment. Timely, accurate and appropriate reimbursement of health care services necessitates comprehensive processes that are well integrated with administrative, clinical and financial systems. CCE provides: a coding system with expert clinical decision logic and integrated references to enable consistent, accurate and complete International Classification of Disease-9-Clinical Modification (ICD-9-CM) or International Classification of Disease-10-Clinical Modification/Procedure Coding System (ICD-10-CM/PCS) and Common Procedural Terminology-4 (CPT-4) coding; editing and grouping software with expected reimbursement (i.e. Diagnosis Related Groups (DRGs), Ambulatory Patient Groups (APGs) and Resource Based Relative Value System (RBRVS)) as well as clinical resource and payer edits for inpatient and outpatient care; compliance with Medicare Code Editor (MCE), National Correct Coding Initiative (NCCI), Outpatient Code Editor (OCE) and Medical Necessity guidelines that address inpatient and outpatient coding compliance issues; and data collection and analysis of patient information and coded data for operational management and performance improvement. All of this reduces errors in the collection cycle.

The CCE application is deployed at 100 host sites supporting 147 CCE instances and is supported and managed by the Solutions Delivery Division (SDD). The CCE application interfaces with CHCS to receive Personally Identifiable Information/Protected Health Information (PII/PHI) from a direct interface to the CHCS system. CCE receives this data to enhance the coders ability to properly "code" procedures rendered. These records are returned to Composite Health Care System (CHCS) application to properly code, classify and index patient encounters. CCE retrieves data for system function but does not modify PII/PHI in any way. CCE stores coded information on encounters, as well as system data in the form of audit logs.

The PII/PHI sent by the CHCS system to CCE:

Name,
Social Security Number (SSN),
Gender,
Date of Birth,
Home/Duty Zip code and country (if provided),
Providers Name
Family Member Prefix (FMP) and
Date of Service (DOS)
Medical Information (record ID of MHS beneficiaries, diagnosis, procedure)

A previously completed PIA was signed on August 1, 2012 and there have only been minor functional enhancement and fixes made to the application since the last PIA. These enhancements include coding updates, commercial software updates, Information Assurance Vulnerability Alert (IAVA) required patch updates and software version upgrades. There have been no major functionality capabilities added to CCE since the last PIA.

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

The privacy risks regarding the validation, use and sharing of the PII/PHI used by the CCE system is that a system user may inadvertently disclose the PII/PHI. Users of the CCE system are required to obtain and maintain an Automated Data Processing (ADP)-II or higher security clearance level. Authority for the exchange of PII/PHI, between the CHCS and CCE systems is covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as part of health care operations by the MHS. The CHCS system, not CCE, is the collection point for the PII/PHI contained in the CCE system. In addition, all MHS CCE users (civilian, military and contractors) are required to take and pass HIPAA training as part of their initial employment/assignment and annually thereafter to continue working with the CCE system.

The following risks were identified with the acceptable corresponding mitigations:

RISK 1: Inadvertent disclosure of PII/PHI to an unauthorized individual while accessing CCE.
MITIGATION: Logical access to the CCE application, server, and workstations is restricted to authorized personnel. Application access is limited to users approved by the hosting facility and protected with smart card authentication. Access to the application is subject to automated audit log recording and archiving for a minimum of one year. Access to application servers is restricted to authorized personnel approved and controlled by the hosting facility and SDD. Access is protected through user authentication and dedicated secure network connections. Application server logs audit access and are retained and archived for a minimum of one year. Tier III support access has the additional protection of the help desk enclave user authentication and access/audit logging which have been validated through FISCAM audits and are retained for a minimum of one year.

RISK 2: Unauthorized system access, unauthorized disclosure of sensitive but unclassified data, damage to software, and unintentional modification of information stored and processed in the system.
MITIGATION: CCE application database security architecture records the actions performed by users to establish accountability and control access to system functions based on assigned permissions and privileges. Most of these safeguards involve no human interaction and operate transparent to the user.

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. The CHCS system initially provides the PII/PHI to the CCE application. CCE uses the PII/PHI to assist the coders. Updated patient records are returned to CHCS. PII/PHI is not updated in or by the CCE application.

☐ **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. Contractor: Planned Systems Incorporated (Arlington, VA)
Contract Language (Section 6, para 6.4.3 “Personally Identifiable Information (PII) and Protected Health Information (PHI)”): The contractor shall comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (P.L. 104-191) requirements, as well as the Department of Defense (DoD) 6025.18-R, "DoD Health Information Privacy Regulation," January, 2003. This includes the Standards for Electronic Transactions, the Standards for Privacy of Individually Identifiable Health Information and the Security Standards. The contractor shall also comply with all Applicable HIPAA-related rules and regulations as they are published and as Government requirements are defined (including identifiers for providers, employers, health plans, and individuals, and standards for claims attachment transactions). Any rules and regulations that are published and/or requirements that are defined after the award date of this contract, that require expenditure of additional contractor resources for compliance may be considered "changes" and will be subject to the changes clause under the contract.

☐ **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.

CCE does not collect PII/PHI directly from individuals; therefore, individuals do not have the opportunity to consent to the collection of their PII/PHI as part of this system. CCE receives PII/PHI from CHCS, which is the collection point for the PII/PHI and provides individuals the opportunity to consent to the collection of their PII/PHI.

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.

CCE does not collect PII/PHI directly from individuals; therefore, individuals do not have the opportunity to consent to the use of their PII/PHI as part of this system. CCE receives PII/PHI from CHCS, which is the collection point for PII/PHI and provides individuals the opportunity to consent to the use of their PII/PHI. Use of this data is permitted under HIPAA.

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.

CCE does not collect PII/PHI directly from individuals.

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.