PRIVACY IMPACT ASSESSMENT (PIA)

For the

Third Party Outpatient Collections System (TPOCS)
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: 151
- ☐ **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 = 007-000006591

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 12

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. 1079b, Procedures for charging fees for care provided to civilians; retention and use of fees collected; 10 U.S.C. 1095, Health care services incurred on behalf of covered beneficiaries: collection from third-party payers; 42 U.S.C. 2651, Recovery by the United States; 28 CFR Part 43, Recovery of Cost of Hospital and Medical Care and Treatment Furnished by the United State; 32 CFR Part 220, Collection from Third Party Payers of Reasonable Charges for Healthcare Services; DoD 6010.15-M, Chapter 3, Medical Services Account; 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.

Third Party Outpatient Collections System (TPOCS) is the DoD standard system designed to assist medical treatment facilities (MTFs) in the collection, tracking, and reporting of data required in the Third Party Collection Program outpatient billing process. TPOCS provides an effective mechanism to MTFs for identifying, recording, billing and collecting reasonable costs for outpatient care. TPOCS supports processing of standard claims which are populated using an electronic interface from on-site systems including the Composite Health Care System (CHCS) and the Ambulatory Data Module (ADM).

The primary use of the system is to create and track Third Party Outpatient Claims that are sent to Insurance Companies by MTF's and clinics. It collects demographic information on patients, patients' insurance information, and the clinical information passed from CHCS concerning that patient's visit. Defense Health Services Systems (DHSS) owns the software but each site has a System Administrator that is responsible for the software and hardware.

The personally identifiable information/protected health information (PII/PHI) collected by the system includes:
- Patient name
- Home Address
- Social Security number (SSN)
- Insurance policy information
- Medical Information (Diagnosis & Procedure info plus Lab and Radiology tests)
- DOB
- Marital status
- Gender
- Spouse Information

The patients are all retirees or family members of active duty and retirees. Data for the system is retrieved via electronic collection from CHCS. Information is retrieved from the CHCS system using one or more elements of PII/PHI.

System Contact:
Director, Patient Accounting Systems
Skyline 3, Suite 900
5201 Leesburg Pike
Falls Church, VA 22041
Tel: 703-575-6779

A PIA for this system was previously signed on 12 December 2008. TPOCS is currently scheduled to be discontinued in FY2014.

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

The data in the TPOCS requires appropriate technical, procedural, physical, and operational safeguards to ensure its continuing confidentiality, integrity, and availability. TPOCS ensures confidentiality of the data by allowing access to data on a "least privilege" basis. Authorized users' have restricted access to specific data objects based on the assigned permissions associated with the user's account.

To minimize privacy risks, users must have a valid CAC and must have physical access given by the site supervisor. They are also required to complete annual Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy training in order to use the TPOCS application. This responsibility is at the site level due to TPOCS being a distributed system. It is the responsibility of the security and privacy individuals at the site level to ensure privacy risks are mitigated and minimal. The TPOCS servers are located in secure computer rooms at the different facilities.

They are controlled by the security controls of that installation.

Users must have an Automated Data Processing (ADP)-II clearance.

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. TPOCS Billing Offices at each MTF

☐ **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. Insurance claims are sent to an external clearinghouse, which reformats the data for presentation to the insurance companies and sponsors' insurance companies.

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.

Individuals cannot object because the collection of their PII/PHI has already been done prior to any PII/PHI being accessed by the TPOCS servers.

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.

Individuals cannot object because the collection of their PII/PHI has already been done prior to any PII/PHI being accessed by the TPOCS servers.

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 TPOCS is a system of records, it is not the initial point of collection for any PII/PHI. Instead, TPOCS receives all PII/PHI from the CHCS. Accordingly, a Privacy Act Statement is not necessary.

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.