



PRIVACY IMPACT ASSESSMENT (PIA)

For the

TRICARE E-Commerce (TMA ECS)

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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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
- 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

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

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; 38 U.S.C. Chapter 17, Hospital, Nursing Home, Domiciliary, and Medical Care; 32 CFR 199.17, TRICARE Program; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); 45 CFR Parts 160 and 164, Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules; 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 Defense Health Agency (DHA) is accountable for the management and operation of the TRICARE program to ensure delivery of military health and private sector care services. In support of the private sector care, DHA has implemented the TRICARE E-Commerce program, which provides an integrated family of applications supporting private sector care contract management and financial management functionality. TRICARE E-Commerce contract management capabilities include healthcare contract solicitation, award, administration, deliverable management, performance management, and operations management. TRICARE E-Commerce financial management capabilities include budget accounting, financial accounting, receivables and payables accounting, healthcare claims payment, and debt collection. E-Commerce applications are secure and maintain transaction records for audit and historical reporting purposes.

In support of contract management, healthcare claims payment, and debt collection, TRICARE E-Commerce receives, maintains, and disseminates personally identifiable information (PII) to include:

Personal descriptors, ID numbers, financial information and life information.

The PII collected pertains to the following categories of individuals: MHS beneficiaries, business partners/ contacts, hospitals, physicians, pharmacies, and other providers.

TRICARE E-Commerce interconnects with the Department of Treasury, Managed Care Support Contractors (MCSCs), the TRICARE Encounter Data (TED), Procurement web sites (e.g., Electronic Data Access (EDA), System for Award Management (SAM), and several banks (i.e., PNC, Bank of America, and Bank One-also known as JP Morgan Chase). E-Commerce can be accessed from more than one site.

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

The system has identified several PII risks and has implemented mitigation approaches:

1) PII within the Oracle Federal Financial (OFF) database (for debt collection) is encrypted. PII within Documentum, and PRISM can remain in the system indefinitely and is not encrypted. Significant OFF, Documentum, and PRISM technical and administrative security measures (e.g., CAC, firewalls, restricted access, etc.) have been adopted to ensure the risks to privacy are minimal. E-Commerce encrypts all sensitive fields in the OFF, Documentum, and PRISM Oracle databases. In addition, an effort is underway to encrypt Documentum content files using vendor proprietary tools.

2) MCSC contract deliverables on Extranet are encrypted and secured once they are uploaded by MCSC personnel (daily). Significant Extranet technical and administrative security measures (e.g., firewalls, IP-restricted access, IP verification, etc.) have been adopted to ensure the risks to privacy are minimal.

3) Files containing PII, transferred between the TED system and E-Commerce to support healthcare claims processing and payment, are encrypted and then temporarily stored on Defense Information Systems Agency (DISA) servers to support data recovery. Significant security safeguards are enforced by elements of the DISA network and server Operating Systems (OS). These safeguards prevent unauthorized access to data files, unauthorized software modifications, and divulgence of confidential processing procedures, techniques or related information. These security safeguards, accomplished through firewalls, network, and server security measures will ensure that the E-Commerce production environment is a secure environment.

4) The system exercises all physical, technical, and administrative controls to protect PII that resides on relational database instances. Best practices are performed and employing techniques that comply with the Information Assurance (IA) guidelines. The E-Commerce applications receive and store PII, collected by other DHA sources, and allow access only to a select group of DHA users for job-related reasons. The selected group of DHA users is

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.

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

PII is not collected directly from the individual. PII is collected from other DHA and MSCS systems for the purposes of processing claims and collecting debt.

However, there is a process in place for an individual to make changes to their information when he/she are in debt with the government. Whenever the Office of General Council (OGC) sends a letter with PII enclosed informing the individual about the debt owed to the government, the individual has the opportunity to call or write to request OGC to correct their PII in the system.

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.

PII is not collected directly from the individual. PII is collected from other DHA or MCSC systems for the purposes of processing claims and collecting debt. Therefore, no consent for these uses is required under DoD 5400.11-R, DoD Privacy Program.

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.

TRICARE E-Commerce does not collect PII directly from individuals. However, OGC provides the following PAS when corresponding with individuals:

AUTHORITY: 10 U.S.C. Chapter 55, Medical and Dental Care; 38 U.S.C. Chapter 17, Hospital, Nursing Home, Domiciliary, and Medical Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); and E.O. 9397 (SSN), as amended.

PURPOSE: To obtain information from an individual that will facilitate an administrative review of a determination of overpayment on a TRICARE health insurance claim.

ROUTINE USES: Information collected may be used and disclosed generally as permitted under 45 CFR Parts 160 and 164, Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, 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, the DoD "Blanket Routine Uses" under 5 U.S.C. 552a (b) (3) apply to this collection. Collected information may be shared with private business entities under contract with the Department of Defense, including CHAMPUS contractors, for the purposes of evaluating claims pricing and payment.

DISCLOSURE: Voluntary. However, if you choose not to provide the requested information, your request for reconsideration may not be approved, and you may experience 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.