



PRIVACY IMPACT ASSESSMENT (PIA)

For the

TRICARE Management Activity E-Commerce (TMA ECS)
--

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
- 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.

TMA ECS includes budgeting, accounting, solicitation, contract administration, business management, and operations to assist TMA personnel in the management of health care contracts and the payment of health care claims. TMA E-Commerce applications are secure and maintain transaction records for audit and historical reporting purposes. TRICARE consolidates the direct health care resources of the Department of Defense and supplements this capability through the use of managed care support contracts and purchased care services.

TMA ECS collects, maintains, and disseminates personally identifiable information (PII) to include:

Name

Social Security Number (SSN)

Sponsor SSN and family member prefix (FMP)

Mailing address

Telecommunications numbers (e.g., mobile, fax, and telephone)

Financial account information and/or numbers

Military status and/or records

Other numbers originated by the government that specifically identify an individual

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

TMA has central administrative and management facilities located in Falls Church, Virginia and Aurora, Colorado. TMA-Aurora is responsible for the managed care support contracts and purchased care services providing the following: the preparation and issuance of health care contracts, the management of health care contract activities, the processing and payment of health care claim invoices, and the recording and reporting of financial transactions. In support of these activities, TMA has implemented the E-Commerce system which serves as a centralized, multi-regional, multi-user, integrated group of applications to manage health care financial and contract management activities. TMA owns the system and MHS operates the system.

TMA ECS consists of the following integrated suite of applications:

1. The TEDS Interface - Financial Management System (TI-FMS) application serves as the interface between the TRICARE Encounter Data (TED) system and E-Commerce functionality using TED file transfers. TI-FMS provides the capability to convert health care claims to invoices, create payment information, process payments, and report on payment details. TI-FMS is a custom built, COBOL based, application executing on a DoD Information Systems Agency (DISA) mainframe computer. When TED files arrive at the mainframe, they contain personally protected information (PII) and protected health information (PHI) (e.g., name, SSN, address, medical, etc.). The TI-FMS application extracts all necessary financial, non-PII/PHI and secures the files. No PII or PHI is maintained in the TI-FMS databases.

2. The Purchased Care Web Site (PCWS) and Contractor Resource Center (CRC) applications provide a variety of TI-FMS financial reports on health care contracts. Users include military and civilian staff members of military treatment facilities, intermediate offices and commands, TMA and uniformed service headquarters, and contractors who support these organizations. PCWS and CRC are custom built applications using Cold Fusion and SQL Server. No PII resides in the PCWS/CRC applications.

3. The Oracle Federal Financials (OFF) application is the core financial application, supporting health care budget and accounting functions. The OFF application supports TMA Contract Resource Management (CRM) for budget and accounting and TMA Office of General Counsel (OGC) for debt management. The OFF application manages the formulation and execution of the current year budget, supports maintenance of the accounting classification structure, and maintains financial records. The OFF application also uses external interfaces to issue payments, provide financial reports, and display management information to other federal government agencies, financial agencies, and financial institutions. The OFF application

modules and data base products execute on DISA Unix platforms. The OFF application maintains PII information (e.g., name, SSN, address, etc.) to support OGC debt management.

4. The Comprizon.Buy application manages TMA health care solicitation and contract administration functions. TMA uses Comprizon.Buy to define requirements for solicitation, conduct a solicitation, and complete an award. Once a contract award takes place, the contract administration function performs management and execution of the contract through its life cycle. Comprizon.Buy is a COTS product that executes on a Windows Platform using the Oracle DBMS. The Comprizon.Buy application may contain PII (e.g., name, SSN, address, etc.) as part of health care contracts.

5. The Management Tracking and Reporting (MTR) application is a custom-built tool that provides a mechanism to track TRICARE program requirement changes through their life cycle and provides operations personnel a consistent and comprehensive ability to document contractor performance. MTR provides for cross platform reporting of information by extracting data from the various applications to provide integrated reporting capabilities. Additionally, the E-Commerce Extranet application supports the ability of Managed Care Support Contractors (MCSC) to submit contract deliverables electronically. The MTR and Extranet applications are custom-built applications that use Cold Fusion with an Oracle DBMS on Windows platforms. No PII resides in the MTR application. The Extranet application may contain PII (e.g., name, SSN, address, etc.) as part of MCSC contract deliverable files. The files are removed from the Extranet application once they are imported into Documentum.

6. The Documentum application is a document content management product that provides search and retrieval, workflow, version control, change control, and document life cycle management functionality. Documentum manages files (e.g., Word and PDF) generated and received in connection with the administration of TMA health care contracts. Documentum uses the Oracle DBMS and executes on Windows platforms. The Documentum application may contain PII (e.g., name, SSN, address, etc.) as part of health care contract and MCSC contract deliverable content.

The system interconnects with the Department of Treasury, Managed Care Support Contractors (MCSCs), the TRICARE Encounter Data (TED) system, and three banks (i.e., PNC, Bank of America, and Bank One-also known as JP Morgan Chase). The system can be accessed at more than one site. TMA ECS is classified as a networked, major application, Sensitive But Unclassified (SBU), Department of Defense (DoD) Mission Assurance Category (MAC) III system.

System contact information:

TRICARE Management Activity E-Commerce System (TMA ECS)
Program Manager, E-Commerce
16401 East Centretech Parkway
Aurora, Colorado 80011
(303) 676-3430

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

The system has assessed several predominant PII risks to include:

1) PII within OFF (for debt collection), Documentum, and Comprizon.Buy remain in the system indefinitely and is not encrypted. Significant OFF, Documentum, and Comprizon.Buy technical and administrative security measures (e.g., CAC, firewalls, restricted access, etc.) have been adopted to ensure the risks to privacy are minimal. In addition, an effort is underway to encrypt all E-Commerce databases.

2) MCSC contract deliverables transferred to the Extranet application are SSL encrypted for transmission. Deliverable files on Extranet are removed from the application once they are imported into Documentum (daily). Significant Extranet technical and administrative security measures (e.g., firewalls, 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 the E-Commerce TI-FMS application to support health care claims processing, are encrypted for transmission and remain on the Defense Information Systems Agency (DISA) mainframe to support data recovery. The TI-FMS security safeguards are enforced by elements from

the application security controls, application security resource access, security provided by the Integrated Document Management System (IDMS) internal security database, the Computer Associates-Top Secret Security (CA-TSS) product, and the mainframe Operating System (OS). These safeguards prevent unauthorized access to data and data files, unauthorized software modifications, and divulgence of confidential processing procedures, techniques or related information. These security safeguards, accomplished through firewalls and network security measures will ensure that the TI-FMS mainframe environment is a trusted 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 system stores PII collected by other TMA sources, which allows access to a select group of TMA users and contractor technical personnel for job-related reasons. TMA users, along with system administrators and contractor technical staff members, are required to complete privacy and Health Information Portability and Accountability Act (HIPAA) training.

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. Department of Treasury - Debt collection actions are initiated by MCSC contractors following contract requirements. For uncollected debts that meet several criteria, the contractors will forward cases to the TMA OGC Claims Collection Section. The Claims Collection Section validates the debts and refers eligible debts to Treasury for further collection action using an OFF application generated statement that notifies the debtor of the referral. The notice directs debtors to contact Treasury with any questions. The computer generated statement includes the following, in addition to the debtor's address:

- a. patient name
- b. debt amount
- c. account number

State and Local Agencies.

Specify.

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

Specify. Managed Care Support Contractors (MCSC)

All contracts contain language which requires the contractor to comply with the HIPAA Privacy Rule and the HIPAA Security Rule. In addition to the responsibilities to comply with the HIPAA Privacy Rule and the HIPAA Security Rule, the contractor is required to comply with the Privacy Rule of 1974, as amended (Privacy Act).

Other (e.g., commercial providers, colleges).

Specify. PNC, Bank of America, and Bank One-also known as JP Morgan Chase. TMA personnel also access bank web sites and download reconciliation information via file transfer protocol (FTP).

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.	<p>The TMA ECS does not collect PII directly from individuals. However, OGC provides the following PAS when corresponding with individuals:</p> <p>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.</p> <p>PURPOSE: To obtain information from an individual that will facilitate an administrative review of a determination of overpayment on a TRICARE health insurance claim.</p> <p>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.</p> <p>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.</p>
----------------------------------	---

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.