



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Cahaba Safeguard Administrators, LLC (CSA) Pharmacy Utilization Management Audit System (PUMAS)

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 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); 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 Department of Defense (DoD) administers an integrated TRICARE Pharmacy Benefits Program which offers pharmacy services to eligible beneficiaries through direct care pharmacies located at Military Treatment Facilities (MTFs) and through purchased care points of service which include a mail order pharmacy and retail network pharmacies or otherwise authorized retail non-network pharmacies under the TRICARE Pharmacy (TPharm) contract.

Under the TRICARE Fraud and Abuse Pharmacy Support (TFAPS) Contract, Cahaba Safeguard Administrators, LLC (CSA) functions as the Fraud and Abuse oversight contractor for TPharm activities including both Mail Order Pharmacy (MOP) services (including specialty pharmacy) and TRICARE retail pharmacy network services. CSA will also perform periodic reviews on behalf of the DoD on other areas of the program at the direction of TRICARE Management Activity (TMA). TMA does not own and will not own the system.

CSA will establish a Memorandum of Understanding (MOU) with the TPharm contractor, Express Scripts, Incorporated (ESI), to obtain an initial data load of TRICARE Retail and Mail Order Pharmacy claims for the previous three years, with monthly updates provided thereafter. Claims will be provided in their National Council for Prescription Drug Program (NCPDP) format. They will be positioned by the TPharm contractor on a secure server at the DoD Pharmacy Operation Center in San Antonio, Texas and downloaded via an encrypted secure transmission to the CSA platform. Note that NCPDP is the Health Insurance Portability and Accountability Act of 1996 (HIPAA) standard for pharmacy claims transactions. Additionally, at a future date, CSA, as the TFAPS contractor will also establish an MOU with Emdeon and use this same process to receive and store data in NCPDP format from Pharmacy Data Transaction Service (PDTS) that will include Pharmacy Data for prescriptions filled at Military Treatment Facilities (MTFs) for Drug Review activities. Upon receipt of these data loads, CSA will perform analyses to check for instances of fraud, waste, and abuse within the TRICARE mail order and retail pharmacy benefit.

The personally identifiable information (PII)/protected health information (PHI) collected by this system includes:

- Name
- Birth Date
- Gender
- Spouse Information
- Child Information
- Medical Information
- Other ID Number (TRICARE Beneficiary ID)

The medical information collected by this system includes both prescription and pharmacy information. Pharmacy information will include name of beneficiary, name of pharmacy, location of pharmacy, amount billed to beneficiary, and beneficiary co-pay amount. Prescription information will include all things on the prescription format, including but not limited to: prescription number, drug name, and the date the prescription was filled. Once the final file format is attained from ESI and Emdeon (PDTS), any additional PII/PHI fields identified will be added to the PIA.

The categories of individuals contained in this system include all TRICARE enrollees that have received pharmacy services through at least one of the three pharmacy points of service (Mail Order, Retail, or MTF Pharmacies). Information collection is required for fraud and abuse oversight activities and other review activities as defined in the TFAPS Statement of Work.

System Contact:

TRICARE Fraud and Abuse Pharmacy Support Contract (TFAPS)
Executive Program Director
375 Riverchase Parkway East

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

CSA has established mitigation plans to prevent privacy risks as well as protocols to report any breaches, in the event that they occur. Mitigations include a secured closed private network, secured work environment, and ongoing compliance training on protecting PII/PHI. Quarterly compliance training will be conducted with CSA TFAPS associates and will include updates and reviews of company privacy policies. This training will be required for all associates working on the TFAPS contract. Any PII/PHI breach or security incident that occurs will be reported immediately upon discovery to the System Privacy/Security Officer, who will then report the breach or incident in accordance with TMA requirements. See also item F below.

CSA has developed a private, secure network and client/server environment which is dedicated to serving DoD operations. It consists of dedicated Sun servers running Solaris and VMware, dedicated desktops and encrypted laptops, all of which are running across an encrypted network. This dedicated client/server environment will support analysts using SAS (an industry leading statistical software and data management solution), SAS Enterprise Miner, SAS Enterprise Guide, Microsoft Office products, DataFlux, and internal CSA applications developed through SAS/IntrNet.

Additionally, all DoD TRICARE data will be stored on a fully encrypted, dedicated Hitachi Storage Area Network (SAN). CSA is currently in the process of completing the DoD Information Assurance Certification and Accreditation Process (DIACAP) for this network, with an anticipated approval date of June 30, 2011. This system is a MAC Level III classified system with a confidentiality level of Sensitive.

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.

TMA – the only information outflow from CSA will be in the form of written Fraud and Abuse referrals to TMA that contain: TRICARE Beneficiary ID, Name, Date of Birth, Gender, Spouse Information, and Child Information. Note that TMA will have these PII/PHI elements in its existing systems.

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.

CSA will have an MOU with ESI and Emdeon. CSA will receive PII/PHI through system-to-system interfaces with ESI initially and PDTS (Emdeon) at a future date. This interchange will be a one-way information exchange as CSA will receive data that includes PII/PHI from ESI and Emdeon (PDTS), but will not share any data back with these DoD contractors.

CSA's contract with TMA contains language that safeguards PII/PHI.

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.

CSA is not the initial point of collection of PII/PHI from individuals; therefore individuals do not have the opportunity to object to the collection of their PII/PHI. CSA receives data from ESI, PDTS (Emdeon), and TMA, all of which collect PII/PHI directly from individuals and provide individuals the opportunity to object at the point of collection.

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.

CSA is not the initial point of collection of PII/PHI from individuals; therefore individuals do not have the opportunity to consent to the specific uses of their PII/PHI. CSA receives data from ESI, PDTS (Emdeon) and TMA, all of which collect PII/PHI directly from individuals and provide individuals the opportunity to consent at the point of collection.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|---|--|
| <input type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input checked="" type="checkbox"/> None |

Describe each applicable format.

CSA is not the initial point of collection of PII/PHI from individuals; therefore no privacy act statement or privacy advisory is needed. CSA receives data from ESI, PDTS (Emedon) and TMA, all of which collect PII/PHI directly from individuals and provide the appropriate notices.

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.