PRIVACY IMPACT ASSESSMENT (PIA)

For the

Pharmacy Data Transaction Service (PDTS)
Defense Health Agency (DHA) / Pharmaceutical Operations Directorate

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: 12846
- ☐ **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 = 007-000001689

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 23

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; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); DoD Instruction 6015.23, Delivery of Healthcare at the Military Treatment Facilities, Foreign Service Care, Third-Party Collection, Beneficiary Counseling and Assistance Coordination (BCACs); 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.

PDTS is a central repository for prescription data from all DoD pharmacy services. PDTS uses a centralized data system to store and analyze information about prescriptions filled across the DoD's network of pharmacies, improving efficiency and patient safety by reducing the likelihood of life-threatening drug interactions involving prescription medications. PDTS carries out extensive clinical editing on prescriptions submitted by TRICARE Pharmacies (TPharm, encompassing both retail and mail-order points of service). These edits include checking the submitted prescription against the patient's medication history for drug/drug interactions, therapeutic duplication and overlap, and over and under-utilization. PDTS also checks for over and under-dosage, and for other conditions specified by DoD, such as edits that restrict specified beneficiaries to particular prescribers and/or pharmacies. PDTS carries out the same edits for prescriptions submitted from over 500 Military Treatment Facilities (MTFs).

The PDTS Medication history includes prescriptions dispensed by TPharm and MTF pharmacies, by Veteran's Administration (VA) pharmacies for dual-eligible beneficiaries, and by in-theater dispensing locations, as reported by the Theater Medical Data Store (TMDS) system. PDTS clinical editing considers all prescriptions when conducting its clinical edits. Neither TPHARM nor the MTF pharmacies have the complete patient medication history; it resides only in PDTS.

PDTS supports the National Council for Prescription Drug Programs (NCPDP) Telecommunications Standard Versions 5.1 and D.0 as formats for claims submission; usage of the NCPDP standard is mandated by HIPAA.

PDTS collects the following types of personal information about information about individuals and must be submitted on all pharmacy claims:

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

PDTS collects, maintains, and disseminates personally identifiable information (PII)/protected health information (PHI) about uniformed services medical beneficiaries enrolled in Defense Eligibility Enrollment Reports Systems (DEERS) who have received prescription drugs from any submitting pharmacy.

DUR (Drug Utilization Review) checking requires that multiple prescriptions for the same patient be evaluated together. PII is required to insure that the proper prescription records are linked for DUR evaluation.

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

There are always potential risks associated with the collection, use, and sharing of PII. Proper measures have been implemented to mitigate and minimize these risks. These include annual 3rd party audits, audits of login activity, monthly vulnerability scans, vulnerability patch management, annually updated contingency plans, "least privilege" access control, user training and awareness, and annual policy reviews.

Because PDTS houses PII and PHI, security clearance is required for every authorized PDTS user. The PDTS team has developed an Incident Response Plan which describes procedures for investigating and reporting security breaches and disclosures of personal information.

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. PDTS discloses information only to DHA and to external parties authorized by DHA as recipients of specific data.

• Medical Data Repository (MDR) for the purpose of advising MDR of dispensing activities.
• Defense Health Service Systems (DHSS) for the purpose of advising DHSS of dispensing activities.
• Composite Healthcare Data Repository (CHDR) for the purpose of advising CHDR of dispensing activities.
• Defense Manpower Data Center (DMDC)/DEERS Immunization Tracking System (HL7IMM) for the purpose of supplying data on immunizations given in retail pharmacies.
• Project ESSENCE for the purpose of advising Project ESSENCE of dispensing activities.

☐ **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. All contracts contain language concerning Privacy Act and HIPAA Privacy and Security compliance for contractors that will access PII/PHI in this system (contract language available upon request).

• ExpressScripts, Incorporated (ESI) for the purpose of advising ESI of Prior Authorizations generated pursuant to dispensing selected drugs at an MTF pharmacy.
• Humana Military Health System (HMHS) for the purpose of advising HMHS of dispensing activities.

☐ **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.

PDTS 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. PDTS receives PII/PHI from other source systems, 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.

PDTS 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. PDTS receives PII/PHI from other source systems, which is the collection point for the PII/PHI and provides individuals the opportunity to consent to the collection of their PII/PHI.

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 PDTS is a system of records, this PIA states that PDTS does not collect personally identifiable information (PII) directly from individuals. Instead, PDTS collects PII from other systems of records through system interfaces. As such, a Privacy Act Statement is not necessary in connection with PDTS.

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.