PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Purchase Care Operating System

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

01/05/24

Solution Delivery Division (SDD)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees
- [x] from both members of the general public and Federal employees
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

Purchase Care Operating System (PCOS) is a multi-module application consisting primarily of the Tricare Encounter Data module (TED) and the Patient Encounter Processing and Reporting (PEPR) module. PCOS provides a method for external medical providers (Managed Care Support Contractors (MCSCs) to submit for reimbursement for care/services to DOD beneficiaries and for internal analysis and quality/ cost control. The PCOS – TED module is the core collection point for DoD purchased care claim related data. Health care providers submit claims to TRICARE for payments of services rendered to TRICARE beneficiaries. The carriers electronically transmit their claims and payment information to TRICARE. (Note: TED is not allowed to replace data in an individual's record. TED cannot make determinations about beneficiaries or employees using this data.) The PCOS – PEPR module, the core reporting hub, is a web-based suite of applications that enables analysis of the purchased care claims and encounter data generated by the TRICARE MCSCs. PEPR provides reporting on data for integration, analysis, compilation, and display of health care claims. It enables analysis and tracking of claims billed at the patient and family level for groups of patients, the provider level for individual professional or institutional providers, and for groups of providers. PEPR also assists in resource sharing opportunities and potential dollars to be recaptured by Military Treatment Facilities (MTFs). It also has a reporting application to analyze the data that it compiles which helps executive and other business analysts make more informed decisions.

The types of personally identifiable information (PII) collected by TED include: personal descriptors, unique identifiers, health information, and life information. The types of PII collected by PEPR include personal descriptors, personal ID numbers (including Social Security numbers), protected health information (PHI), medical information, and contact information.

PCOS receives data from the following categories of individuals: military personnel, dependents, and retirees.

The sites accessing the system are located at Managed Care Support Contractors (MCSCs) operations and DHA locations.
PCOS is owned and operated by the Defense Health Agency (DHA) Solution Delivery Division (SDD), Clinical Support Program Office (CSPMO) (DAD IO / J-6).

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

PII/PHI in PEPR is collected to verify the correct information is being processed for an individual regarding claims data (i.e., payment reimbursement), health care data reporting, fraud and abuse detection, and contractor performance monitoring. The intended use of PII/PHI collected is to: process an individual's claim after verifying one's identity, charge the appropriate procedure code, generate a comprehensive health report, and detect fraud.

PII/PHI is collected in TED because it is the minimum amount of PII/PHI required to efficiently and effectively process a purchase care claim. The intended use of PII/PHI collected is to ensure that the following mission-related goals for TED and DHA/MHS are met:
• Claims are tracked immediately after submission

• Payment claims are validated within three days
• Claims reimbursement is efficient
• Electronic claims processing is streamlined
• Claims acceptance is automated
• Claims are processed within hours

Claim information required for fraud and abuse litigation will be shared by the DHA Program Integrity (PI) Office with the Defense Criminal Investigative Services (DCIS) for legal/litigation purposes and with the Defense Information Systems Agency (DISA) for system administration purposes.

e. Do individuals have the opportunity to object to the collection of their PII? ☐ Yes ☒ No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Individuals do not have the opportunity to object to the collection of their PII because PEPR and TED is not the initial point of collection.

f. 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 do not have the opportunity to consent to the specific uses of their PII because PEPR/ TED is not the initial point of collection.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☐ Privacy Act Statement ☐ Privacy Advisory ☒ Not Applicable

PCOS does not collect PII directly from individuals. Therefore, no Privacy Act Statement or Advisory is required.

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	DHA Program Integrity (PI) Office, DHA Contract Resource Management (CRM) Division, DHA SDD BoXi Common Services (BCS)
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Claim information required for fraud and abuse litigation will be shared by the DHA Program Integrity (PI) Office with the Defense Criminal Investigative Services (DCIS) for legal/litigation purposes and with the Defense Information Systems Agency (DISA) for system administration purposes. Note: all DISA contractors have secret clearances.
☐ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	
☐ State and Local Agencies	Specify.	

☒ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	Support contractors with access to PII/PHI include: Planned Systems International (PSI) and Koniag- GS and Alquimi Contractors who access the PCOS application are also required to provide a valid Data Sharing Agreement (DSA). All contracts contain language which require the contractor to comply with the HIPAA Privacy Rule and the HIPAA Security Rule. In addition, the contractor is required to comply with the Privacy Act of 1974, as amended. The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect all Government data. The Contractor shall also ensure the confidentiality, integrity, and availability of Government data in compliance with all applicable laws and regulations, including data breach reporting and response requirements, in accordance with DFAR Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoDD 5400.11, "DoD Privacy Program," May 8, 2007, and DoD 5400.11-R, "DoD Privacy Program," May 14, 2007. The contractor shall also comply with federal laws relating to freedom of information and records management. To protect PII, all contractors are responsible for the employment of practices that satisfy the requirements and regulations of the following: Section 208 of E-Government (E-Gov) Act of 2002, (Pub. L. 107-347); DoDI 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," February 12, 2009; and, Office of Management and Budget (OMB) Memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 26, 2003. Under DoD Manual 6025.18, "Implementation of the HIPAA Privacy Rule in DoD Health Care Programs," March 13, 2019, reasonable steps must be taken to implement appropriate procedural, administrative, technical and physical safeguards to prevent the unauthorized use and/ or disclosure of any personally identifiable information (PII) or PHI. Likewise, all uses, disclosures, and destruction of PII and PHI data are generally subject to DoD 5400.11-R, "DoD Privacy Program," May 14, 2007, as well as DoDI 8500.2, "Information Assurance (IA) Implementation," Feb. 6, 2003, and DoD 8580.02-R, "DoD Health Information Security Regulation," July 12, 2007. Data is shared with MTFs, MCSCs, and subcontractors who are within the MHS organization or under MHS contracts. (Note: tier 3 contractors are required to undergo the Clinical Support personnel security process and have annually refreshed DD Form 2875 on file.) Note: DoDI 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019, reissued and canceled DoDD 5400.11; DoDI 8500.2 was canceled by DoDI 8500.01, "Cybersecurity," March 14, 2014; and DoD 8580.02-R was canceled by DoDI 8580.02, "Security of Individually Identifiable Health Information in DoD Health Care Programs," August 12, 2015.
☐ Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☐ Individuals	☐ Databases
☒ Existing DoD Information Systems	☒ Commercial Systems

☐ Other Federal Information Systems

Existing DoD Information Systems - MHS Data Repository (MDR)
Commercial Systems - 3M (PEPR Tier III support vendor) and information systems owned by commercial insurance companies with purchased care contracts with the DHA

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

☐ E-mail
☐ In-Person Contact
☐ Fax
☒ Information Sharing - System to System
☐ Other *(If Other, enter the information in the box below)*
☐ Official Form (*Enter Form Number(s) in the box below)*
☐ Paper
☐ Telephone Interview
☐ Website/E-Form

Data is collected from external Commercial Systems via the Military Health System (MHS) Enterprise Infrastructure/DISA Business to Business (B2B) gateway.

Data is collected from MDR via direct interface over the MHS Virtual Private Network (VPN).

k. 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 must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier EDTMA 04

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. GRS 3.1, item 012 (DAA-GRS-2013-0005-0008)

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

FILE NUMBER: 1601-11
DISPOSITION: Temporary. Cut off and destroy when related master file or database has been deleted.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must 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) Privacy and Security Rules; and E.O. 9397 (SSN), as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

PCOS is not the initial point of collection of information.