PRIVACY IMPACT ASSESSMENT (PIA)

For the

Purchased Care Operations System (PCOS) – Patient Encounter Processing and Reporting (PEPR)
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**	☐	**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	140 (EI/DS)
☐	**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: 007-000000510 (EI/DS)

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 EDTMA 04

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) 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 Patient Encounter Processing and Reporting (PEPR) system is a web-based suite of applications that enables analysis of the purchased care claims and encounter data generated by the TRICARE Managed Care Support Contractors (MCSCs), and is the core reporting point for Military Health System (MHS) purchased care claim-related data. PEPR provides reporting on data for integration, analysis, compilation, and display of health care claims in order to analyze and track 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).

Personally identifiable information (PII) and protected health information (PHI) collected by PEPR include:

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

PEPR receives data resulting from purchased care encounters from military personnel, dependents, and retirees.

Defense Health Agency (DHA) will own the requirements to the system. MHS will operate the system. The system will be accessed at one or more sites and will host a web site that is Common Access Card (CAC)-enabled and not accessible to the public. The sites accessing the system will be located at MCSC operations and DHA locations.

PEPR is managed under the Defense Health Services Systems (DHSS) Program Office.

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

The privacy risks associated with PII / PHI collected include the mishandling of PII / PHI by authorized users of the system.

To mitigate these risks, PII / PHI in PEPR is protected with appropriate physical, technical, and administrative safeguards to ensure its continuing confidentiality, integrity, and availability in accordance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 Privacy and Security Rules.

The privacy rights of beneficiaries and employees will be protected by ensuring access is only granted to authorized users who are required to have a sponsor to fulfill the standard DHSS procedures for gaining access to application data and functionality. Proper paperwork (DD Form 2875, System Authorization Access Request) is processed and vetted before access is granted to the system.

PEPR is vetted through the DoD Information Assurance Certification and Accreditation Process (DIACAP) and multiple audits.

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. DHA

☒ **Other DoD Components.**

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) and with the Defense Information Systems Agency (DISA) for system administration purposes.

Note: all DISA contractors have secret clearances.

☒ **Other Federal Agencies.**

Specify. Department of Justice (DoJ); Judge Advocate General (JAG)

☐ **State and Local Agencies.**

Specify.

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

Specify. Planned Systems International (PSI) and General Dynamics Information Technology (GDIT)

The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and 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.

Data are 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 DHSS personnel security process and have annually refreshed DD Form 2875 on file.)

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.

☐ **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.

PEPR 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.

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.

PEPR 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.

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.	PCOS – PEPR does not collect personally identifiable information (PII) directly from individuals. Instead, PCOS – PEPR receives PII from other systems of records. Accordingly, a Privacy Act Statement is not necessary in connection with PCOS – PEPR.

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.