PRIVACY IMPACT ASSESSMENT (PIA)

For the

TRICARE Managed Care System (TRIMACS)
TRICARE Management Activity (TMA)/Managed Care Support Contractor (MCSC)

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 DTMA 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 MHS Beneficiaries

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 C.F.R. 199 (TRICARE Prime and TRICARE Program); 45 C.F.R. Parts 160 and 164, Health Insurance Portability and Accountability Act Privacy and Security Rules; E.O. 9397 (as amended, SSN); and DoD 5400.11-R, Department of Defense Privacy Program.

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.

TRICARE Managed Care System's (TRIMACS) purpose is to provide claims processing and related support services for persons with dual TRICARE and Medicare eligibility in support of the Department of Defense (DoD) TRICARE program. The role of the contractor is to assist the Defense Health Program in operating an integrated health care delivery system by providing claims assistance and by processing specified TRICARE claims for payment.

The information collected from providers includes patient demographics such as name, address, Social Security Number (sponsor number) and date of birth. Other medical information collected involves diagnosis, procedure codes for medical services received, and occasionally medical records for processing (i.e. to determine medical necessity). The category of individuals' (patients') information being collected could be active duty and/or their dependents, retirees and/or their dependents, foreign nationals, former spouses, reservists, and National Guard personnel. TMA owns the data, Wisconsin Physicians Service (WPS) owns the system, and TMA has a contract with WPS to process medical claims for the TRICARE Dual-Eligible Fiscal Intermediary Contract (TDEFIC).

System contact information:
Director of Contract Compliance
1707 W. Broadway
Madison, WI 53713
(608) 301-2299

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

There is a risk of unauthorized personnel accessing TRIMACS or any connected system. Another risk is an unauthorized person trying to remove hard copy data from work areas. The system is secured by DoD Information Assurance Certification and Accreditation Process (DIACAP) to avoid penetration from an outside entity.

There is also potential for a provider or individual to try and gain access to personally identifiable information (PII)/ protected health information (PHI) via the web. A provider or individual could try to gain access to information to which they are not entitled by misrepresenting themselves. A beneficiary has to be valid against the Defense Enrollment Eligibility Reporting System (DEERS) in order to register on the portal. Once the beneficiary agrees to the "terms and conditions", they are asked to enter their personal contact and security information for validation with DEERS and their password applying WPS's password requirements based on DoD guidelines. If the validation with DEERS and the password are successful, the beneficiary will be taken to the registration process for completion. Following the registration confirmation, if an address is not on DEERS or the patient record, the user will be required to enter an address to build a patient file. Once the information is supplied for registration, an e-mail is sent to the user to complete their registration by following the link given in the e-mail. After this is completed the beneficiary has access to their records.

A provider must agree to the "terms and conditions" before registering on the portal. The provider has the option to register with a domestic or international address. For domestic addresses, they are required to enter the Medicare number, license number or national provider identifier (NPI). The provider's tax identification number and zip code are validated against the provider file on the claims processing system. Once a valid provider is found within the search, the provider is taken to the registration process. This step of the registration process gives providers the option to have instant access, or wait for a temporary password to be sent by postal mail to the physical address in the provider file. If the users would like instant access they are required to provide claim verification. The user must enter two different claim numbers for two different patients. The claim numbers cannot be on the same TRICARE Explanation of Benefits (TEOB). This information is validated against the WPS's claims processing system.

During the provider registration process a user name and password is created (the password must follow the WPS and DoD password rules). Once the information is supplied and saved for registration, an e-mail is sent to the users to complete their registration by following the link given in the e-mail, which allows the provider to have access to the portal. If providers are the first to register for the tax identification number and zip code given, they are registered as the administrator for that site. Otherwise they will be registered as a normal provider user.

The system access is restricted on an as needed basis. Each building has a security guard and/or swipe card access and every employee is required to have a badge as well as an automatic data processing ADP level I or II security clearance under DIACAP. WPS also completes an annual audit of controls.

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 TRICARE Encounter database in Oklahoma City, Oklahoma. This data is exchanged via the Business-to-Business (B2B) Gateway between WPS and Oklahoma City.

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. When requested from Judge Advocate General (JAG) or US attorneys offices, WPS shares information on medical claims processed via e-mail redacting the Social Security Numbers (SSN). WPS provides to the Center for Medicare and Medicaid Services' (CMS) Coordination of Benefits Contractor (COBC), information for patients for whom WPS wants to receive medical claims information. This data exchange is via Network Data Mover (NDM) which is a file transfer product commonly employed to transfer files between mainframe computers and midrange computers.

☐ **State and Local Agencies.**

Specify.

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

Specify. WPS has a signed Memorandum of Understanding (MOU) with TriWest Healthcare & Humana Military Health Services. WPS has also submitted an MOU to HealthNet Federal Services for which a signature is pending. In the MOU, it states that all data transferred between the contractor and WPS will be in compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administration Simplification Rules and Chapter 21 of the TRICARE Operations Manual (i.e., protecting PII/PHI whether it is in paper/electronic format or using National Provider Identifiers (NPIs), and providing HIPAA training for staff). WPS transmits claims data to TriWest through a secured connection and transmits claims data to Humana and HealthNet via the NDM.

All contracts contain language which require the contractor to comply with the HIPAA, 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 Act of 1974.

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

Specify. WPS sends Explanation of Benefits (EOBs) to beneficiaries and providers that provide medical services to TRICARE beneficiaries via U.S. postal service or they can sign into the secured portal.

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.

Information from the beneficiary is voluntary. The individual has a choice whether or not to submit their claims for payment to WPS. If the individual submits their claims, they are required to submit PII/PHI in order to process the claim under the correct individual, make claim payments to the individual or provider, and to provide the required information to the government.

(2) If "No," state the reason why individuals cannot object.

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.

PHI is collected for permitted uses and disclosures as set forth in DoD 6025.18-R, DoD Health Information Privacy Regulation. Individuals are informed of these uses and WPS documents disclosures. Individuals are given the opportunity to restrict the use or disclosure of their PHI based on the procedures in place at the local facility where the data is collected and maintained, in accordance with DoD 6025.18-R, C10.1.

The Privacy Act of 1974 and DoD Regulation 5400.11-R allows individuals to authorize to specific uses of their PII. If an individual does not complete an Authorization to Disclose Information Form, WPS will not release PII for specific uses. If an individual refuses payment for a claim submitted for payment, they can send the check back to WPS or sign the check over to the provider of care. Consent to the specific uses of PII is obtained as necessary, in accordance with DoD 5400.11-R, DoD Privacy Program, C4.1.3.

When information is released outside of routine uses, authorization is required. For example, if a beneficiary would like their medical records released to an attorney, all information is completed on the Authorization to Disclose Information Form on file. When an individual requests information, WPS can verify the Authorization to Disclose Information Form and release claim information.

When an individual ask WPS to release information, WPS will send a written request to the involved party asking permission to release medical claims information, to whom the information can be released to, and how long the release is in effect. When WPS ask an individual for PII/PHI for processing their claim, this

request is completed via U.S. Postal Service with a letter included (that has the Privacy Act Statement listed).

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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.

Privacy Act Statement:

AUTHORITY: 44 U.S.C. 3101; 10 U.S.C. 1079 and 1086; 38 U.S.C. 1781; E.O. 9397.

PRINCIPAL PURPOSE(S): To evaluate eligibility for medical care provided by civilian sources and to issue payment upon establishment of eligibility and determination that the services/supplies received are authorized by law.

ROUTINE USE(S): Information from claims and related documents may be given to the Department of Health and Human Services and/or the Department of Homeland Security consistent with their statutory administrative responsibilities under CHAMPUS; to the Department of Justice for representation of the Secretary of Defense in civil actions; to the Internal Revenue Service and private collection agencies in connection with recoupment claims; and to Congressional offices in response to inquiries made at the request of the person to whom a record pertains. Appropriate disclosures may be made to other federal, state, local, foreign government agencies, private business entities, and individual providers of care, on matters relating to entitlement, claims adjudication, fraud, program abuse, utilization review, quality assurance, peer review, program integrity, third-party liability, coordination of benefits, and civil and criminal litigation related to the operation of CHAMPUS.

DISCLOSURE: Voluntary; however, failure to provide information will result in delay in payment or may result in denial of claim.

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.