PRIVACY IMPACT ASSESSMENT (PIA)

For the

United Healthcare Military & Veterans Information System
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

☐ **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	OMB approval request to occur shortly
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); 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 United Healthcare Military & Veterans Information System (hereafter referred to as "the System") is a set of technology and applications used to administer the Managed Care Support Contract in support of TRICARE beneficiaries in the West Region. TRICARE provides health care services for military personnel, including some members of the National Guard and Reserve Components, military retirees, and their family members. The System is used to provide the services including the following:

• Enrollment
• Billing
• Referral
• Authentication and Authorization
• Clinical services
• Call center support
• Waste, fraud, and abuse detection/investigation
• Compliance violation detection/investigation, include those involving waste, fraud, abuse and privacy violations
• Medical management
• Self-service tools for beneficiaries and providers

The System may contain personally identifiable information (PII) about the following:
• Active Duty Service Members and their families
• National Guard and Reserve Members and their families
• Retired Service Members and their families
• Retired National Guard and Reserve Members and their families
• Dependent Parents and Parents-in-Law
• Foreign Force Members and their families
• Former family members of any of the above

The Personally Identifiable Information (PII) / Protected Health Information (PHI) about individuals collected in the systems are:

Personal descriptors, ID numbers, health, financial, employment, life, and education.

The program is owned and operated by the UnitedHealthcare Military & Veterans.

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

The risks associated with the PII collected are as follows:

- There is a risk of someone gaining an individuals PII while in transit. This risk is mitigated by implementation of FIPS 140-2 encryption and a written policy that all PII requires encryption.

- There is a risk of improper handling of PII by untrained employees and contractors. This risk is mitigated by a requirement that all employees and contractors attend training on the proper handling and usage of PII.

- There is a risk that someone without an authorized need to know could access PII data that is stored on the system or on archive tapes. This risk is mitigated by access control processes, procedures designed to track tapes containing PII, use of monitoring tools and disciplinary action for violating company policies.

- There is a risk associated with employees and contractors violating company policy and using PII for unintended or illegal purposes. This risk is mitigated by thorough background investigations, use of monitoring tools and a mature incident response process.

United Healthcare Military and Veterans has appointed a privacy officer to lead the privacy compliance program. The contact information for the privacy officer is below:

Chief Privacy Officer
UnitedHealthcare Military & Veterans
9800 Health Care Lane
Minnetonka, MN 55343
mvprivacy@uhc.com

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. TRICARE Regional Office (TRO), Defense Health Agency (DHA), Military Treatment Facilities (MTFs)

☒ **Other DoD Components.**

Specify. Defense Manpower Data Center (DMDC)

☒ **Other Federal Agencies.**

Specify. Federal Law Enforcement Agencies

☒ **State and Local Agencies.**

Specify. State Attorney General Offices, State Law Enforcement Agencies

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

Specify. Palmetto Government Benefits Administrators - (PGBA), SourceHOV, Optum

All contracts with subcontractors contain language that require them to comply with DoD regulations and all applicable federal, state and local laws including the HIPAA Privacy Rule, the HIPAA Security Rule, and the Privacy Act.

☐ **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.

PII/PHI contained in the System is collected voluntarily. Individuals may object to or restrict the collection of their PII/PHI verbally, in writing, or in person. If an individual chooses not to provide their information, no penalty may be imposed, but absence of the requested information may result in administrative delays or the inability to process an individual's request.

(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.

Individuals are given the opportunity to consent to the specific uses of their PII. Consent is obtained as necessary in accordance with DoD 5400.11-R, Department of Defense Privacy Program, C.4.1.3. 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 are given the opportunity to authorize or restrict the use 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.

(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.

This statement serves to inform you of the purpose for collecting personal information required by the UnitedHealthcare Military & Veterans Information System and how it will be used.

AUTHORITY: 10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); and E.O. 9397 (SSN), as amended.

PURPOSE: To collect information from you in order to manage your TRICARE enrollment, provide your benefits, and/or pay for those services.

ROUTINE USES: Your records may be disclosed to investigate waste, fraud, abuse, security, and privacy concerns. Use and disclosure of your records outside of DoD may also occur in accordance with the DoD Blanket Routine Uses published at http://dpclo.defense.gov/privacy/SORNS/blanket_routine_uses.html and as permitted by the Privacy Act of 1974, as amended (5 U.S.C. 552a (b)).

Any protected health information (PHI) in your records may be used and disclosed generally as permitted by the HIPAA Privacy Rule (45 CFR Parts 160 and 164), as implemented within DoD. Permitted uses and disclosures of PHI include, but are not limited to, treatment, payment, and healthcare operations.

DISCLOSURE: Voluntary. If you choose not to provide your information, no penalty may be imposed, but absence of the requested information may result in administrative delays or the inability to process your request.

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.