PRIVACY IMPACT ASSESSMENT (PIA)

For the

Health Net Federal Services Information System
TRICARE Management Activity (TMA) / Managed Care Support Contractor

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

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); 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 Health Net Federal Services (HNFS) Information System is a Contractor Owned/Contractor Operated (COCO) system dedicated to administering the Managed Care Support Contract in support of Military Health System (MHS) beneficiaries. 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 HNFS Information System includes enrollment; authorization; referral; medical management; call center support; self service via a publicly accessible website and secure web portal; waste, fraud, and abuse (WFA); retrospective review (RRS); and services for health care providers.

The HNFS secure web portal provides beneficiaries in the TRICARE North Region with information including, but not limited to: information about enrollment, claims, covered benefits, payments, referrals, and authorizations. Beneficiaries access this information by logging into the portal via username and password; the secure portal is located on the Health Net Federal Services web site (hnfs.com). Once logged into the portal, beneficiaries are able to view the status of submitted claims and authorizations, submit electronic enrollment forms, make enrollment payments, find participating providers, etc. Additionally, beneficiaries have the ability to view and print paper forms used for the purposes of collection, use, disclosure, processing, retention and destruction of personally identifiable information (PII)/protected health information (PHI).

The secure web portal can also be accessed by providers as a means to obtain information including, but not limited to: beneficiary authorization status, beneficiary cost-share and co-payment amounts, beneficiary referral status, and summaries of covered benefits. Providers can also submit beneficiary authorizations, referrals, and claims through the portal.

HNFS has subcontracted some of the services in the North Region to include PGBA, LLC, Cognizant Technology Solutions U.S. Corporation and SourceHOV, LLC to maximize efficiencies. This PIA covers the HNFS portions of the North Region Contract systems only. It is inclusive of privacy risks, and controls for data stored and managed in HNFS, including applications and subsystems which are dependent and integrated with the PGBA information system managed by PGBA.

The PII/PHI collected by this system includes:
• Name
• Other Names Used
• Social Security Number (SSN)
• Truncated SSN
• Other ID Number
• Gender
• Birth Date
• Cell Telephone Number
• Home Telephone Number
• Personal Email Address
• Mailing/Home Address
• Spouse Information
• Martial Status
• Child Information
• Financial Information
• Medical Information
• Law Enforcement Information
• Employment Information
• Military Records
• Ethnic Origin
• Race
• Language
• Fax Number

The HNFS Information System covers all types of MHS beneficiaries including 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, survivors, children, Medal of Honor Recipients and their families, Unremarried Former Spouses, Dependent Parents and Parents-in-Law, Foreign Force Members and their families, family of Court Martialed Sponsor, family of Sponsor Missing in Action, and victims of abuse.

System contact:
HNFS TRICARE Program
Manager, IT Security
12033 Foundation Place
Rancho Cordova, CA 95742

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

As a contractor for the TRICARE North Region, HNFS upholds the responsibility to ensure the privacy of all data maintained for the government. HNFS has a Business Associate Agreement in place and owns the responsibility to ensure the Privacy and Security of the PII/PHI of TRICARE beneficiaries. HNFS is required to comply with not only Department of Defense (DoD) specific Privacy rules, but also those promulgated by Federal Laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and other Federal Agency regulations such as those published by the Social Security Administration, Health and Human Services, and the Internal Revenue System, as well as the laws and regulations of state and district authorities in Connecticut, Delaware, the District of Columbia, Illinois, Indiana, Kentucky, Maine, Maryland, Massachusetts, Michigan, New Hampshire, New Jersey, New York, North Carolina, Ohio, Pennsylvania, Rhode Island, Vermont, Virginia, West Virginia, Wisconsin and portions of Iowa (Rock Island Arsenal area) and Missouri (St. Louis area).

The HNFS Information System is subject to the same privacy risks as those of similar systems engaged in the health insurance business, namely:
• Unauthorized or improperly authorized access/disclosure of PII/PHI
• Inadequate or ineffective protection processes
• Third party access/disclosure

The consequences of a loss of privacy are also the same as for any other health insurance business, including:
• Legal liability
• Financial liability
• Reputation loss
• Business loss
• Trust loss

These risks and consequences are addressed by HNFS through a combination of policies and procedures for collecting and protecting confidential data such as why collect, what to collect, who collects, collection context, and who has responsibility for the data.

PII/PHI contained in the system is specifically classified, assigned an owner, and governed by business rules for use and retention. A comprehensive protection plan is in place that includes personnel awareness training for all users to include initial and annual training required to perform assigned Security and Privacy responsibilities, individually traceable auditing of actions undertaken within the system, authentication and authorization for all access, change and configuration management of the system, and technical measures such as data separation (the process of splitting the data into different categories and storing these data categories separately), encryption of data in transit, the deployment of firewalls, intrusion detection, and data loss prevention systems. The protection scheme is regularly assessed for compliance with HNFS and DoD policy and guidance.

All authorized Information System (IS) users (including contract and training personnel) receive initial and annual security awareness training along with initial and refresher privacy and security training.

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. The HNFS Information System shares data with TRICARE Management Activity (TMA), Military Treatment Facilities (MTFs), and DoD personnel or individuals acting on behalf of the DoD whose security has been cleared by the DoD and whose access to PII/PHI is consistent with health care operations as defined by HIPAA and The Privacy Act of 1974, as amended.

☒ **Other DoD Components.**

Specify. Defense Manpower Data Center (DMDC)

☒ **Other Federal Agencies.**

Specify. Law enforcement as required to support Waste, Fraud, Abuse or Security and Privacy Incident Response Investigations

☒ **State and Local Agencies.**

Specify. Law enforcement as required to support Waste, Fraud, Abuse or Security and Privacy Incident Response Investigations

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

Specify. Contracts with all sub-contractors (e.g. IBM, AT&T, PGBA) that have access to PII/ PHI contain language that states that these businesses must establish the roles and responsibilities for sharing information. Additionally, all contractors must implement and maintain security and privacy safeguards in accordance with the DoD directives prior to accessing or connecting to the HNFS Information System and ensure that appropriate safeguards are implemented for the confidentiality, integrity, and availability of the connected systems and the data they store, process, and transmit.

All sub-contractor access and connection must be managed to continuously minimize community risk by ensuring that the assurance of one IS is not undermined by vulnerabilities of a connected IS. All personnel with physical or logical access to the HNFS Information System including those of its subcontractors have obtained the appropriate clearance from the TMA Personnel Security Division, demonstrated a need-to-know, and have signed Security, Privacy, Acceptable Use and other such non-disclosure agreements.

All contracts contain language that requires the contractor to comply with the HIPAA Privacy Rule and 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.

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. TRICARE Customer Service associates will attempt to retrieve the individual's information by alternative means if applicable.

(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.

Individuals may submit an Authorization for Disclosure of Medical or Dental Information, Request to Restrict Protected Health Information, or other appropriate legal documentation.

(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.	The Privacy Act Statement will appear at or before the point PII is collected from TRICARE beneficiaries enrolled or requesting to be enrolled with TRICARE, in a conspicuous manner, regardless of the medium used for collection. This statement serves to inform you of the purpose for collecting personal information required by Health Net Federal Services, on behalf of the TRICARE Program, and how it will be used. AUTHORITY: 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); 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 occur in accordance with the DoD Blanket Route 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. The following Privacy Act Statement (PAS) may be provided in lieu of the above PAS when collecting PII from an individual over the telephone. If the individual requests to know more about the authorities or routine uses, that section of the above PAS should be read. If the individual requests a paper copy of the PAS, the individual may choose whether to withhold any responses until a paper copy of the above PAS has been provided. I am about to request information from you in order to manage your TRICARE enrollment, provide your benefits, and/or pay for those services. 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. The authorities permitting this collection include 10 U.S.C. Chapter 55 and 38 U.S.C. Chapter 17. Your information may be disclosed to investigate waste, fraud, abuse, security, and privacy concerns. It may also be disclosed to support the reason you called today, and other reasons compatible with why it was collected, if permitted by the HIPAA Privacy Rule and other applicable privacy laws. Would you like to know more about the authorities or routine uses, or receive a paper copy of the full Privacy Act Statement?

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.