PRIVACY IMPACT ASSESSMENT (PIA)

For the

Humana Military Healthcare Services Automated Information Systems (HMHS)
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. 1079 and 1086; 38 U.S.C. Chapter 17; 32 CFR Part 199; 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 purpose of Humana Military Healthcare Services (HMHS) is to validate the eligibility of beneficiaries and refer them to physicians for medical treatment, authorize care, pay claims, assign beneficiaries to physicians for Prime benefits, and facilitate informational contact with beneficiaries. The individuals from whom personal information is collected are military personnel and/or their dependents, retirees and/or their dependents, contractors, former spouses, Reservists, and National Guard personnel.

HMHS uses information already in existence and collects information to verify user's identity and grant access to the website. Personally identifiable information (PII)/protected health information (PHI) is used to verify identity, grant access, and provide services available through HMHS and includes: name, Social Security Number (SSN), gender, date of birth, home telephone, e-mail address, mailing/home address, spouse information, marital status, child information, and medical information.

Other PII collected include the following:

Beneficiary - relationship to sponsor, sponsor branch of service, sponsor retirement confirmation, retired, user identification (ID) created, password, reminder question/answer, and the security agreement acceptance.

Provider - user ID, password, password question/answer, work email, work phone, work fax, supervisor name, supervisor phone, role with provider, company name, company address, city, state, zip code, company email, and the security agreement acceptance.

Government - military base, title, work phone, work fax, work email, supervisor, password, password question/answer, and the security agreement acceptance.

System point of contact:
Humana Military Privacy Official
500 West Main Street 19th floor
Louisville, KY 40202
hmhsprivacyoffice@humana.com
502-580-1621

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

Privacy risks are: (1) unauthorized access to the servers, (2) disclosure of an individual's PII/PHI to individuals without a valid need-to-know, and (3) accidental disclosures.

1) The risk of unauthorized access to the HMHS servers is addressed in detailed policy and procedures, as well as Department of Defense (DoD) Information Assurance Certification Accreditation Process (DIACAP) reviews and accreditation. To safeguard privacy, multiple security access layers have been developed to reduce the possibility of unauthorized access and minimize the impact if compromised by an attacker. Physical access to the HMHS servers/ data center is controlled via 24/7 roving security. User name and passwords are needed to access sensitive information. These passwords adhere to the DIACAP requirements for complexity, auditing, and 60 day change requirements.

2) The risk of disclosure of an individual's PII/PHI to individuals without a need to know is addressed to safeguard privacy by requiring Humana personnel to have an automatic data processing (ADP-II) certification and setting up users' security on a need to know role basis.

3) The risk of accidental disclosure of an individual's PII/PHI is addressed through an active management program with provider representatives. Processes within this program are designed to minimize the risk of selecting the

wrong provider which includes a process that requires using the last beneficiary address used by the provider. Every time an accidental disclosure occurs, the totality of the processes and systems are reassessed to determine if improvements can be made.

Aggressive actions for improvement are continuously taken. For example, reduction of PII/PHI collected on documents (e.g., remittances, referrals, etc.) has been accomplished. In addition, the full SSN has been removed from the remittance.

Individual privacy is protected by requiring all Humana personnel take extensive annual privacy trainings. Privacy risk assessments are completed within every department of HMHS annually. HIPAA and privacy trainings takes place to address privacy risks and refresher privacy trainings are conducted throughout the year. HMHS maintains a DoD Information Assurance Certification and Accreditation Process (DIACAP) Authorization to Operate (ATO) with annual reviews.

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. Defense Enrollment Eligibility Reporting System (DEERS) with TRICARE Regional Office (TRO), and TRICARE Management Activity (TMA).

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify. Developers/Contractors - HMHS occasionally use contractors for development and maintenance of software within HMHS. All contractors are required to complete the online Ethics and Privacy training, and the HMHS Essentials training.

HMHS and the contracting company (i.e., Professional Management Enterprises, Inc.) are required, based on the "Master Service Agreement" (Article 7: Confidentiality; and EXHIBIT E - Health Insurance Portability and Accountability Act (HIPAA) BUSINESS ASSOCIATE ADDENDUM), not to disclose information. Contractors complete and sign access security forms and are granted system access in a similar manner to Humana personnel. Access to data is governed through a security controlled system with DIACAP compliant audit trails in place. Contractor work performance and productivity is monitored by a Humana manager.

All contracts contain language which requires the contractor to comply with 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, 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.

The PII collected through the web site is strictly voluntary for beneficiaries. They can elect to either obtain access to the Online Beneficiary Services or have TRICARE materials mailed to their address. Individuals may decline when asked if they want to provide/update certain information (i.e., personal email address) on file. If they do not voluntarily provide their email address, they will not receive electronic communications from HMHS. Instead all communication will be provided through the United States (U.S.) Mail.

HMHS collects a limited amount of PII during web page registration. HMHS uses this information to verify the user against DEERS. HMHS has placed the Privacy Act Statement on the web site as requested by the TMA Privacy Office.

Information collected is used to verify identity and usage of the website. Providing the information is voluntary. However, if the user fails to provide the requested information, HMHS will not be able to verify the identity of the user. If the identity is not verified, the user will be unable to gain access to the website. Other uses and disclosures must be authorized by the individual.

(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.

Beneficiaries can refuse to provide PII. However, available services may not be able to be provided.
PII collected on the web site is strictly voluntary for beneficiaries. During the web user self-registration, individuals will view the Privacy Act Statement prior to entering any user information into the user self-registration. At that time, individuals can give consent by clicking "Continue".

If beneficiaries want to receive electronic communications from HMHS, they must voluntarily provide consent when interfacing with the web user self-registration portal. If they do not voluntarily elect/consent to obtain access to Online Beneficiary Services, they will not receive electronic communications from HMHS and their TRICARE materials will be mailed to their address through the U.S. Mail.

PII is only used and disclosed to validate the eligibility of beneficiaries and refer them to physicians for medical treatment, authorize care, pay claims, assign beneficiaries to physicians for Prime benefits, for informational contact with beneficiaries, and other healthcare operations. PII collected by Humana is not used for marketing or research purposes.

(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.

AUTHORITY: 10 U.S.C. 1079 and 1086; 38 U.S.C. Chapter 17; 32 CFR Part 199; 45 CFR Parts 160 and 164, Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules; and E.O. 9397 (SSN), as amended.

PURPOSE: To obtain information from individuals to validate their eligibility as beneficiaries, grant access to the HMHS website, and provide beneficiary services available through HMHS to validated individuals, including physician referrals, healthcare authorizations, claims payment, assignment of beneficiaries to physicians, and informational contact with validated beneficiaries.

ROUTINE USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records may be specifically disclosed outside the Department of Defense as a routine use under 5 U.S.C. 552a(b)(3) as follows: to the Departments of Health and Human Services and Homeland Security, and to other Federal, State, local, and foreign government agencies, private business entities under contract with the Department of Defense, and individual providers of care, on matters relating to eligibility, claims pricing and payment, fraud, program abuse, utilization review, quality assurance, peer review, program integrity, third-party liability, coordination of benefits, and civil or criminal litigation.

DISCLOSURE: Voluntary; however, failure to furnish all requested information will result in an individual not being able to access beneficiary services available through the HMHS website.

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.