PRIVACY IMPACT ASSESSMENT (PIA)

For the

TRICARE ONLINE (TOL) 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: 142
- ☐ **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 007-000006593

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 EDHA 07

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.

Authorities: 10 U.S.C. Chapter 55, Medical and Dental Care; 45 CFR Parts 160, General Administrative Requirements and 164, Security and Privacy; DoD 6025.18-R Health Information Privacy Regulation; 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.

TRICARE Online (TOL) is the Department of Defense (DoD) online patient portal providing eligible beneficiaries access to military hospital and clinic appointing, prescription (Rx) refill, DoD Blue Button personal health data (PHD), Secure Messaging (SM), Service Separation/Retirement and Nurse Advice Line (NAL).

DoD beneficiaries age 18 years or older, including active duty service members, retired service personnel and their families, can use TOL Patient Portal (TOL PP) services and information. Beneficiaries can securely access information using their DoD Common Access Card (CAC), DoD Self-Service Logon (DS Logon) Premium (Level 2) and Defense Finance and Accounting Services (DFAS) myPay (Level 2) credentials.

TOL PP capabilities are available 365/24/7 from any Defense Information Systems Agency (DISA) allowable location via approved Internet Service Provider (ISP). TOL PP provides convenient access to online tools which empower patients to be more active participants in their health care. TOL PP saves time, money and frustration.

Key Capabilities:
> Appointing services for an authorized/authenticated user and/or authorized family member(s)
- Schedule primary care and select self-referral military hospital or clinic appointments.
- Cancel, view, and/or print past and future appointments
- Receive up to three email and/or text reminders for appointments
> Rx Refill for an authorized/authenticated user and/or authorized family member(s)
- Request Rx refills and status information
- Receive Rx Refill(s) request confirmations
> DoD Blue Button for an authorized/authenticated user and/or implicit child(ren) under 12 years old:
- Access DoD personal health data including medications, allergies, problem lists, encounters, lab results, radiology results, vital signs and immunizations

Key Benefits:
- Consolidates existing patient health care capabilities
- Provides convenient 365/24/7 self service
- Provides secure login with DoD CAC, DS Logon Premium, or DFAS myPay
- Encourages active participation in health care
- Increases beneficiary access to care
- Reduces the administrative workload for military hospitals and clinics
- Reduces appointment no show rates
- Increases patient satisfaction
- Saves resources, time and money

TOL PP is designed using open architectural standards. The system uses the existing Defense Information System Network (DISN) and currently available commercial infrastructure. TOL PP is a common portal that helps to ensure appropriate privacy policies and mechanisms are in place, provides an enterprise security solution, and helps to address the Health Insurance Portability and Accountability Act (HIPAA), Section 508 of the 1998 Rehabilitation Act, and other regulatory requirements.

TOL PP receives from Defense Manpower Data Center (DMDC), via the MHS iAS, the authenticating user's PII: Electronic Data Exchange Personal Identifier (EDI_PI); first, middle, & last name; social security number (SSN); date of birth (DOB); gender; branch of service (if applicable); affiliating rank (if applicable); and sponsor's SSN (if applicable) as captured in the DMDC Defense Enrollment Eligibility Reporting System (DEERS) as a means of authenticating the identity of the end user prior to granting access to TOL PP.

TOL PP receives from DMDC, via the MHS iAS, the family member(s) attributes (if applicable) along with authenticating user's PII: EDI_PI; first, middle,& last name; DOB; branch of service (if applicable); affiliating rank (if applicable); Status; and benefit associated as captured in DMDC DEERS as a means of associated

family members to authorized users. Family member(s) age 18 or older must authorize release of information within DEERS for TOL PP to receive/display.

TOL PP collects, as provided by the Authenticated User, e-mail address (up to three) and personal cell numbers (up to three) if the TOL PP user elects to obtain appointment reminders and/or prescription refill notifications.

TOL PP collects, as provided by the Authenticated User, numeric prescription numbers to requests a prescription refill for themselves or authorized family member if the TOL PP user elects to request a prescription refill using prescription numbers.

TOL PP collects, as provided by the Authenticated User, the military treatment facility (MTF) for appointing services and/or pharmacy dispensing location for prescription refill pickup if the TOL PP user elects to utilize the appointing and/or prescription refill capabilities.

TOL PP transmits PII to DES for AHLTA CDR data retrieval when a user requests to view their PHD data using the DoD Blue Button.

TOL is owned by Defense Health Agency (DHA) and managed under the Solutions Delivery Directorate (SDD) Clinical Services Program Office:
SDD Clinical Support Program
5109 Leesburg Pike
Sky 6, Suite 817
Falls Church, VA 22041
(703) 882-3876

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

RISK: Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule requires the MHS to provide its patients and beneficiaries a Notice of the MHS' Privacy Practices (MHS NoPP).

MITIGATION: TOL PP provides the HIPAA required MHS NoPP via a prominent link on the TOL Log on page.

RISK: TOL Patient Portal user may not understand what risks may be present to their PII and how what safeguards are in place to address those risks.

MITIGATION: TOL PP posts 'Accessibility and Security' for user reference on each page consisting of following sections:
Privacy and Security Policy
Privacy Act Warning
Security of Information
Family Members and Privacy
Login
Logging Out
The Use of Cookies
Exit Site Notice
Surveys, Questionnaires, and Polls
Changes to This Policy
Accessibility / Section 508
Medical Disclaimer
Blue Button Disclaimer
Appointment Reminder Disclaimer

Sections in detail:

Privacy and Security Policy

We know that privacy and security of information matters to you. We respect your privacy and have taken measures

to provide appropriate levels of security to protect your personal information. We will never release your name, street address, telephone number, e-mail address or any other personal information to unauthorized users. We deploy computer security technology to protect any information you provide to us.

Privacy Act Warning

Information contained in this system is subject to the Privacy Act of 1974 (5 U.S.C. 552a, as amended). Only authorized persons in the conduct of official business may use personal information contained in this system. Any unauthorized disclosure or misuse of personal information may result in criminal and/or civil penalties. Any official or employee may be found guilty of a misdemeanor and fined not more than $5,000.00 if he or she willfully discloses personal information to anyone not entitled to receive information. Any individual may file a civil action against a Department of Defense (DoD) component or its employees if the aggrieved individual feels that certain provisions of the Privacy Act have been violated. An aggrieved individual may obtain the payment of damage, court costs, and attorney fees in some cases.

TRICARE Online is a web site of the Military Health System. The Office of the Assistant Secretary of Defense, Health Affairs (HA)and the TRICARE Management Activity provides (TMA) provides it as a public service. Information presented on this site is considered public information and may be distributed or copied unless otherwise indicated. Use of appropriate byline/photo/image credits is requested.

For site management, information is collected for statistical purposes. This government computer system uses software programs to create summary metrics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration General Schedule 20. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 (Pub. L. 99-474, Oct. 16, 1986, 100 Stat. 1213).

Department of Defense Security Notice and Consent Banner TRICARE Online (TOL) is a Department of Defense (DoD) computer system. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. government use. DoD computer systems may be monitored for all lawful purposes, including ensuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. Authorized DoD personnel may monitor all information, including personal information, placed or sent over this system.

Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or civil action.

Security of Information

At all times, security maintenance and administration is an essential element of web site operation and maintenance. TRICARE online (TOL) employs several levels of security to protect the personal identifiable information of registered users. In addition, these security levels are anticipated to be in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191, Aug 21, 1996,110 Stat. 1936).

•Eligibility Verification - In order to achieve the appropriate levels of security, the account creation process uses security software that receives the user's demographic data (i.e....., date of birth, Social Security Number, and name) from the Defense Enrollment Eligibility Reporting System (DEERS) during the authentication process. DEERS determines the user's eligibility for using certain features of TOL by making sure that the user is an eligible TRICARE beneficiary.
•Secured Socket Layer (SSL) - A security protocol, which provides a transmission level of encryption between the user's browser and TOL server machines. SSL is a method for protecting a TOL user's identification.

Family Members and Privacy

Some states have restrictions on disclosure of health information to family members to protect the privacy of certain minors and dependent adult family members. These restrictions on disclosure of information may include accessing personal health and medical information through electronic or Internet based services. If you have questions regarding this matter, we recommend that you contact your local Military Treatment Facility or the Defense Enrollment Eligibility Reporting System Support Office for more information about disclosure of health information and applicable privacy laws within the state or jurisdiction that you and your family receive care.

Login

TRICARE Online (TOL) requires users to login to access services included but not limited to make an appointment for you or your family members, refilling a prescription for you or your authorized family members, viewing your personal health data via Blue Button, or communicating electronically with your health care provider. When you use these services, TOL will clearly disclose what information is required and what information is optional. However, the information you provide is subject to the security and privacy measures described in this policy.

Logging Out

You should remember to log out when you are finished accessing TOL PP. This prevents someone else from accessing your personal information if you leave, share, or use a public computer (e.g....., library, kiosk, or Internet cafe) and your session hasn't automatically "timed out" or shut down.

The Use of Cookies

Cookies may be categorized as session or persistent, which describes the length of time that they stay on your system. The following are detailed descriptions of how we use these cookies.

Session Cookies
A session cookie is a small piece of textual information that a server places temporarily on your browser during the time your browser is open. The cookies are erased once you close all browsers. We use session cookies in the following manner:

•Logon and log-off administration: : When you log on to TRICARE Online (TOL), for example, to use one of our online services, session cookies help with the logon and log-off process. The cookies enable us to recognize your logon identification when you log on so that we do not need to establish your identity for every request.
•Transactions and site usability - We use session cookies to improve how you navigate through the TOL website and conduct transactions. As examples, session cookies are used to maintain your online session as you browse over several pages; to store and pre-populate information so that you do not have to reenter the same information twice.

Persistent Cookies

A persistent cookie is a small piece of text stored on your computer's hard drive for a defined period of time, after which the cookie is erased. TRICARE Online does not use persistent cookies.

Exit Site Notice

TRICARE Online (TOL) has links to many other federal agencies. In a few cases we link to private organizations, with their permission. Once you link to another site, you are subject to the privacy and security policy of the new site. When TOL links to external Internet sites, it does so by opening a new window (or browser) on your screen. Any information in these secondary windows (browsers) should be considered external to the TOL website, and TOL and the DoD are not responsible for its content.

Surveys, Questionnaires, and Polls

To improve the quality of our service, TRICARE Online (TOL) may use surveys, questionnaires and polls to facilitate feedback and input from our end users. When you respond to surveys, questionnaires or polls related to our site, we may, at times, ask you for demographic information such as your age or gender. This information is collected only as anonymous, aggregated information and is used for statistical purposes. Otherwise, we do not collect or store your

personal responses.

Note: TOL PP only utilizes the DoD Interactive Customer Evaluation (ICE) web-based tool to collect user provided feedback on services provided by TRICARE Online (TOL).

Changes to This Policy

This privacy and security policy may be revised periodically. When we make a significant change that affects our collection and use of your personal information or our security and privacy policy, we will post a notice on the TRICARE Online (TOL) home page for thirty (30) days. The most recent changes to the security and or privacy policy will be highlighted in a different color within the policy. We recommend that you read the policy whenever you visit the TOL site in case you missed our notice or have not previously registered for a TOL service or feature.

TOL partners with select third parties to provide you with quality health information and a personalized medical record. We recommend that you read privacy and security policies of these third party partners before using their tools and services.

Accessibility / Section 508

The U.S. Department of Defense is committed to making its electronic and information technologies accessible to individuals with disabilities in accordance with Section 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended in 1999.

If you have concerns related to the accessibility of this website, please Contact Us.

For more information about Section 508, please visit the DoD Section 508 Website.

Medical Disclaimer

TRICARE Online (TOL) is a web-based health information and communication service provided by the Department of Defense (DoD) and contains information from various content providers. As used in the TOL Medical Disclaimer and Agreement ("Agreement"), "We", "Us", or "Our" refers to TOL. "You" or "User(s)" refers to TOL users.

Below is the TOL end-user medical disclaimer and agreement. Here, you will find important information regarding TOL, the terms of user account creation,, and use of TOL.

The terms and conditions of this medical disclaimer and agreement may change from time to time. Such modifications will take effect immediately upon posting on the website. You are advised to review this agreement periodically for changes and modifications.

The information provided by TOL is based on current medical literature and on physician review; however, the information is not intended nor implied to be a substitute for professional medical advice. Nothing on TOL is intended to be used for or replace the advice of your doctor, medical diagnosis or treatment. As always, seek the advice of your physician or other qualified health care provider before starting new treatment or when you have questions regarding a medical condition or disease. The information provided by TOL is intended to help people make better health care decisions and take greater responsibility for their own health.

BY LOGGING INTO THIS SITE, YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT NEITHER WE NOR OUR SUPPLIERS ARE RESPONSIBLE FOR THE RESULTS OF YOUR DECISIONS RESULTING FROM THE USE OF TOL, INCLUDING, BUT NOT LIMITED TO, YOUR CHOOSING TO SEEK OR NOT TO SEEK PROFESSIONAL MEDICAL CARE, OR YOUR CHOOSING OR NOT CHOOSING A SPECIFIC TREATMENT BASED ON THE INFORMATION PROVIDED BY THIS ONLINE SERVICE.

Blue Button Disclaimer

NOTICE: The use of this application constitutes acceptance of the following terms and conditions.

The use of the TRICARE Online (TOL) Blue Button application on personally owned or publicly accessible, non-government furnished equipment, is at the discretion of the individual user. The Department of Defense assumes no liability in the event of loss or compromise of personally identifiable data, resulting from the use of this

application on non-government furnished equipment.

Your Blue Button data contains Protected Health Information (PHI) from your Electronic Health Record (EHR). Your PHI is not distributed or shared with other users. All Medical Disclaimer and Policy conditions listed above apply. If you need to review these terms and conditions, you may do so through the available links at the bottom of this page.

The TOL Blue Button application incorporates security safeguards to ensure the privacy of your PHI. It is your responsibility to keep your PHI safe. Only you have access to your PHI and as such, you must consider carefully and take full responsibility for disclosure of your account to other individuals.

Changes to this agreement will be distributed to TOL Blue Button users as the information is updated. When you first access the Blue Button, you will be asked to acknowledge that you understand the terms and conditions of use for the Blue Button application.

All Disclaimers listed on the TOL website apply. If you need to review these Disclaimers, you may do so through the available links at the bottom of this page.

Changes to this agreement will be distributed to TOL Blue Button users as the agreement is updated.

Appointment Reminder Disclaimer

You may request text and email message reminders for either your booked or canceled appointments or for your authorized family members. The reminder message will include appointment information, such as you or your family member's name, the date and time of the appointment, and the clinic where the appointment is scheduled.

Appointment reminders are optional. You can elect to receive or decline appointment reminders within your TOL profile. By electing to receive appointment reminders you confirm understanding that the use of any text and or email communications are not secure and that information could be intercepted during transmission by a third party. If you wish to receive appointment reminders, then the appointment information will be sent to the mobile phone number or email address you specify. TOL does not assume responsibility for any related messaging charges.

RISK: Inadvertent disclosure of PII or PHI to an unauthorized individual while accessing the TOL system.

MITIGATION: Clearly define who has access, and what the limits of that access are for all personnel using or maintaining the TOL workstations and LAN, if employed at your site. A logbook of LAN maintenance and other functions is kept next to the server, which includes the following information:
• Person accessing the server
• Function performed (software used, maintenance, network analysis, etc.)
• Time of access

Per HIPAA requirements, each site must ensure that all of the above indicated audit/log information is retained for a minimum of six years.

RISK: Unauthorized system access, unauthorized disclosure of controlled unclassified information (CUI), damage to software, and unintentional modification of information stored and processed in the system.

MITIGATION: TOL application database security architecture records the actions performed by users to establish accountability and control access to system functions based on assigned permissions and privileges. Most of these safeguards involve no human interaction and operate transparent to the user. There are three primary automated security features implemented by the TOL application and the computer's operating system.
1. Discretionary Access Control (DAC): DoD minimum security requirements state that access to information is to be controlled on a discretionary basis. The DAC security mechanism enables access to objects according to the assigned role of the user. All users access the Portal via a Web browser. The Web server serves Hypertext Markup Language (HTML) and Java Script Page (JSP) back to the user's browser. TOL is an object based system. As an object based system, ownership and access to all objects that include files and programs are controlled by the TOL system. Individual users are granted privileges to access certain files based on their inclusion within a specific group. Registered TOL Web site users include beneficiaries and TOL administrators/managers. The System Administrator (SA) for TOL has access to the system components as required for system administration, maintenance and monitoring. Only the TOL system administrator has direct access to the operating systems, databases and network

controls. TOL Web site is configured to restrict unregistered users access to restricted functions on the Web site. Authorized users access the TOL Web site via a Web browser. To gain authorization, users must use their DoD Common Access Card (CAC), DoD Self-Service Logon (DS Logon) Premium (Level 2) and Defense Finance and Accounting Services (DFAS) myPay (Level 2) credentials. Upon registration, a user becomes part of one or more groups. All beneficiaries can register providing that they have a valid DEERS account. Once registered with TOL, they can log on and get access to the beneficiary functions. TOL managers/administrators also register with using one of the aforementioned credentials; however, the designated TOL administrator must activate their account in order to access those Web site functions available only to managers.
2. Identification and Authentication (I&A): I&A safeguard requires each user to positively identify themselves by using their DoD CAC, DS Logon Premium (Level 2) and DFAS myPay (Level 2) credentials. All users can register providing that they have a valid DEERS account. I&A safeguard serves as the mechanism for associating a specific user with the recorded audit events. The TOL Information System Security Manager (ISSM) ensures that I&A defaults and proper authentication parameters are used for all accounts.
3. Auditing: Audit safeguards provide user accountability by recording the events initiated by each individual user. This security service establishes accountability for security-relevant actions and events in the current version of TOL. Audit trails are established to identify the users and processes responsible for the initiation of security-relevant events. All security-relevant actions against the TOL system must be traceable to a single user who is accountable for those actions. To the maximum extent possible, the TOL system must ensure the originator of a file, message, or process can be proven and not spoofed. The use of audit trails, date-time stamps, and future digital signature technology assists in this goal. Auditing is accomplished in three functional areas, Solaria, Oracle Application Server, and Microsoft Windows Server. Each of the three functional areas captures security relevant events and stores them for review by the ISSM.

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. -

☐ **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.

☐ **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.

TOL PP is not a mandated system. An Individual may object to the TOL PP collection of PII by not utilizing the system as the individual's PII is populated by DMDC and AHLTA CDR upon log in.

Users may elect not to receive reminders by not providing their email and phone numbers.

(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.

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

Consent to the specific uses of PII is obtained as necessary, in accordance with DoD 5400.11-R, DoD "Privacy Program", C4.1.3.

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 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, C10.1.

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 AUTHORITY: 10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR Part 199, Civilian Health and

each applicable format.	Medical Program of the Uniformed Services (CHAMPUS); and E.O. 9397 (SSN), as amended. PURPOSE: To allow you to view and manage you and your family's appointments at military hospitals and clinics, refill prescriptions, and view your personal health data through TRICARE Online. ROUTINE USES: Your records may be disclosed to the Department of Veterans Affairs for determining benefits and providing care, as well as to certain other federal agencies to facilitate research and analysis. 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/SORNsIndex/BlanketRoutineUses.aspx 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.

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.