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.

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.

TRICARE Online (TOL) is an online patient-focused portal that provides eligible Department of Defense (DoD) beneficiaries and their families convenient anywhere, anytime access to military healthcare services that support participation in their healthcare experience via a user friendly, network-centric platform. TOL enables beneficiaries online access to manage (schedule, change, and cancel) personal and family appointments at their military hospital or clinic to include receiving email and/or text message appointment reminders; schedule prescription refills for themselves and/or family members for military hospital or clinic pick up; view their personal health data (PHD) via the Blue Button; and access to useful links for TRICARE health and benefits information as well as other useful healthcare information.

In addition to active duty and retired service personnel and their qualified dependents, TOL benefits the entire Military Health System (MHS). TOL technologies help alleviate the administrative healthcare workload, increase access to care, and improve patient satisfaction by automating consolidated healthcare information and services online providing an alternative to limited call center days/times. TOL engages MHS beneficiaries as partners in their own healthcare and helps to improve military healthcare overall by supporting the safety and accuracy of personal healthcare data, avoiding the duplication of tests and reducing delays in treatment.

TOL 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 core capabilities are:

• Appointment Center: Authorized beneficiaries can schedule, cancel and or view future appointments for themselves or an authorized family member(s) and may also elect to schedule appointment reminders via email and/or text messages.

• DoD Blue Button: Authorized beneficiaries can view their own personal health data (PHD) as documented in the MHS and Department of Veteran Affairs (VA) Electronic Health Records (EHR). PHD displays are read-only and the user may print, download this data via the 'Blue Button' capability in a Portable Document Format (.pdf), Text File (.txt) formatted file, or Continuity of Care Document/C-32 (.xml) format, or elect to share with a Direct address recipient. Blue Button displays are view only and NOT retained. TOL does not store any of the data within the TOL system after the user's session has ended.

• Prescription (Rx) Refill: Authorized beneficiaries can request refills of available prescriptions and or check the status of their and authorized family member(s) prescriptions. Single or multiple (up to 10) prescription refills may be requested. Upon accessing this page, the user’s primary military hospital or clinic will be displayed. The user will have the option of selecting an alternate region/military hospital or clinic for their Rx refill. Beneficiaries can also link conveniently to the TRICARE Pharmacy Program webpage.

Personally identifiable information (PII) collected about individuals include: first & last name; social security number (SSN); date of birth (DOB); branch of service (if applicable); e-mail address; personal cell and home telephone numbers; and sponsor's SSN (if applicable) during the authentication process with Defense Manpower Data Center (DMDC) via the MHS iAS. Electronic Data Exchange Personal Identifier (EDI_PI) is obtained from Defense Manpower Data Center (DMDC).

TOL is owned by DHA and managed under the Defense Health Services Systems (DHSS) Program Office.

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

RISK: Inadvertent disclosure of PII or protected health information (PHI) to an unauthorized individual while

accessing TOL .

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.

1. Display of Personal Identifier to end user is limited to last 4 SSN.

2. 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 sensitive but unclassified data, 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.

2. Identification and Authentication (I&A): I&A safeguard requires each user to positively identify themselves by a unique user-identification and password, prior to being granted system access.

3. Auditing: Audit safeguards provide user accountability by recording the events initiated by each individual user.

RISK: Authorized TOL users who retrieve their personal health data via TOL may inadvertently leave their PII on the computer they used to access the information.

MITIGATION: Users must acknowledge understanding as stated in the following warning display prior to downloading their PII information: "WARNING: The file you are about to download contains personal health data. Personal health data on DoD systems is subject to privacy and security safeguards established by DoD and the Health Insurance Portability and Accountability Act (HIPAA). However, these privacy and security safeguards do not apply to personal health data you printout or download and save to the hard drive or other data storage devices available to the computer you are currently using to access TOL. When you log out of TOL or close your browser, any personal health data you downloaded and saved is not deleted; instead it remains on the hard drive or storage device you selected. BE CAREFUL! By downloading or printing personal health data, you acknowledge your responsibility to protect and otherwise secure that data. You also acknowledge that DoD is not responsible for safeguarding the privacy or security of personal health data you print out or save to the selected data storage device. Please take care to protect the confidentiality and integrity of your downloaded personal health data."

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. TOL interfaces to the following external systems:
• AudioCare for Rx Refill services
• Bi-Directional Health Information Exchange - AHLTA (BHIE-AHLTA) for Blue Button displays
• BHIE-DoD Adaptor for Blue Button displays

• Composite Health Care System (CHCS) for appointing services

☒ **Other DoD Components.**

Specify. • DMDC DEERS for authentication services via MHS iAS

☐ **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. An authorized TOL user can can view, print, download (.pdf or .txt or CCD format), and share their PHD using the Blue Button capability once authenticated into TOL. Upon selection, the user will be presented with a dialog box containing warning text and three selection buttons. Warning message text:

"WARNING: The file you are about to download contains personal health data. Personal health data on DoD systems is subject to privacy and security safeguards established by DoD and the Health Insurance Portability and Accountability Act (HIPAA). However, these privacy and security safeguards do not apply to personal health data you printout or download and save to the hard drive or other data storage devices available to the computer you are currently using to access TOL. When you log out of TOL or close your browser, any personal health data you downloaded and saved is not deleted; instead it remains on the hard drive or storage device you selected. BE CAREFUL! By downloading or printing personal health data, you acknowledge your responsibility to protect and otherwise secure that data. You also acknowledge that DoD is not responsible for safeguarding the privacy or security of personal health data you print out or save to the selected data storage device. Please take care to protect the confidentiality and integrity of your downloaded personal health data."

If the user selects either the “Save as Text” or “Save as PDF” button, the TOL system will present a “File Download” window that allows the user to either open or save the requested file. The user also has the option to cancel the process.

If the user elects to Share their PHD with a trusted recipient via Direct services, then the following disclaimer will be presented for user to acknowledge:

"NOTICE: The TRICARE Online (TOL) Blue Button Share application allows you to electronically share personal health information in your electronic health record with individuals and organizations outside the Military Health System (MHS) and Department of Defense (DoD). These non-DoD recipients may include yourself, family members or private healthcare providers, who

would receive your information by email. Whether to use Blue Button Share for this purpose, and who receives your information, are choices made by you, not DoD or the MHS.

The electronic transmission of your personal information through Blue Button Share is believed to be secure, but security cannot be guaranteed. By your use of Blue Button Share, you assume various risks. For example, your personal health information might be lost in transmission to your intended recipient, disclosed by that recipient to someone else you did not intend, or viewed by a hacker who obtains access to the recipient's computer system.

By using Blue Button Share, you acknowledge that neither DoD nor the MHS is responsible for safeguarding against the risks of sharing your personal health information with non-DoD recipients. When you first use Blue Button Share, you will be asked to acknowledge that you understand and agree to these terms and conditions.

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. "

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 is not a mandatory use system and submission of PII is voluntary. Individuals may object to the collection of their PII by not providing information needed to access the system. If the individual chooses not to provide their PII, the individual will not be able to log into TOL and will not have access to TOL services. Instead, users may elect not to use the online system and request similar services directly from their healthcare provider/facility.

(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.

TOL is not a mandatory use system and submission of PII is voluntary.

- Individuals may object (withhold consent) to the collection of their PII by not providing information needed to access the system. If the individual chooses not to provide their PII, the individual will not be able to log into the web site and will not have access to TOL services.
- Individuals may object (withhold consent) by not requesting (selecting) any/all service offerings within TOL. If the individual chooses not to provide their PII, the individual will not be able to log into TOL and will not have access to TOL services. Instead, users may elect not to use the online system and request similar services directly from their healthcare provider/facility.

(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.

TOL is a system of records that collects personally identifiable information (PII) from other systems and directly from individuals. Therefore, a Privacy Act Statement (PAS) should be provided to individuals prior to collecting their PII for inclusion in TOL. A PAS for use with TOL is attached below.

The PAS should be in a conspicuous manner, at or before the point that PII is collected, regardless of the medium used for collection. When PII is collected via a web page, the PAS should be prominently placed on a web page which will be shown to the user before that PII is collected. It should not be provided via a pop-up or hyperlink which can be bypassed or ignored depending on browser settings.

Privacy Act Statement

This statement serves to inform you of the purpose for collecting personal information required by TRICARE Online 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 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.

DISCLOSURE: Voluntary. If you choose not to provide your information, no penalty may be imposed, but you will not have access to the services and benefits of the website.

Warning Notice and Consent to Monitor

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS you consent to the following conditions:

- The USG routinely monitors communications occurring on this IS, and any device attached to this IS, for purposes including, but not limited to, penetration testing, COMSEC monitoring, network defense, quality control, and employee misconduct, law enforcement, and counterintelligence investigations.
- At any time, the USG may inspect and/or seize data stored on this IS and any device attached to this IS.
- Communications occurring on or data stored on this IS, or any device attached to this IS, are not private. They are subject to routine monitoring and search.
- Any communications occurring on or data stored on this IS or any device attached to this IS may be disclosed or used for any USG-authorized purpose.

Security protections may be utilized on this IS to protect certain interests that are important to the USG. For example, passwords, access cards, encryption or biometric access controls provide security for the benefit of the USG. These protections are not provided for your benefit or privacy and may be modified or eliminated at the USG's discretion.

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.

Blue Button Share Disclaimer

NOTICE: The TRICARE Online (TOL) Blue Button Share application allows you to electronically share personal health information in your electronic health record with individuals and organizations outside the Military Health System (MHS) and Department of Defense (DoD). These non-DoD recipients may include yourself, family members or private healthcare providers, who would receive your information by email. Whether to use Blue Button Share for this purpose, and who receives your information, are choices made by you, not DoD or the MHS.

The electronic transmission of your personal information through Blue Button Share is believed to be secure, but security cannot be guaranteed. By your use of Blue Button Share, you assume various risks. For example, your personal health information might be lost in transmission to your intended recipient, disclosed by that recipient to someone else you did not intend, or viewed by a hacker who obtains access to the recipient’s computer system.

By using Blue Button Share, you acknowledge that neither DoD nor the MHS is responsible for safeguarding against the risks of sharing your personal health information with non-DoD recipients. When you first use Blue Button Share, you will be asked to acknowledge that you understand and agree to these terms and conditions.

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 cancelled 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.

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.