



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

TRICARE Online (TOL) System
-----------------------------

TRICARE Management Activity (TMA)
-----------------------------------

### **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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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

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; 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.

TRICARE Online (TOL) increases access to care for the beneficiary, optimizes the provision of care by the provider, and assists in population health while optimizing the business management of the Military Health Systems (MHS). TOL provides the 9.6 million DoD beneficiaries with a single, efficient, cost-effective, user-friendly, network-centric platform that enhances the access and delivery of health care from any location, at any time. The vehicle, or strategy enabler, to achieve these goals is a common, MHS-wide Internet portal focused on providing patient centric services. TOL targets shore-based facilities, although it is accessible to ships that have Internet connectivity, to enable Navy Fleet use. It reduces the redundancy of individual Service and medical treatment facility (MTF) efforts and optimizes the beneficiary's ease of navigation through the MHS.

Beneficiaries can receive access to care through an online capability to schedule and manage appointments, refill and reorder prescriptions, access approved health content, and view their healthcare through personal health data displays. Beneficiaries are able to obtain accurate TRICARE information on services and benefits, claims, enrollment, and TRICARE pharmacy services.

TOL is designed using open architectural standards. The system uses the existing Defense Information System Network (DISN) and currently available commercial infrastructure. 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.

The current release provides the following services:

- Integration with MHS Single Sign-on (SSO) framework known as Identity Authentication Services (iAS)
- Online primary care and self referral appointing capability
- Pharmacy Refill (Rx Refill)
- Online Health Risk Assessments (Health Assessment Review Tool (HART))
- Personal Health Record (PHR) Data
- External website links, e.g. Family Health Portrait, Beneficiary Web Enrollment, etc.

Planned TOL enhancements:

3rd Qtr FY11 Releases:

- Redesigning of HART to Consolidated Health Assessment Review Tool (CHART)
- Access to eForms

4th Qtr FY11 Releases:

- Access to Secure Messaging software as a service (SaaS) capability

Personally identifiable information (PII) collected about individuals include: username; password; first & last name; social security number (SSN); date of birth (DOB); branch of service (if applicable); affiliating rank (if applicable); e-mail address; personal cell and home telephone numbers; and sponsor's SSN (if applicable) during new user registration (via the MHS iAS) to match to data stored in Defense Enrollment Eligibility Reporting System (DEERS) as a means of authenticating the identity of the end user. Electronic Data Exchange Personal Identifier (EDI\_PI) is obtained from Defense Manpower Data Center (DMDC) via iAS.

Authorized TOL users have the ability to check the status of their prescriptions and request refills of those prescriptions that are refillable. From the Refill Prescription page, single or multiple prescription refills may be requested. Upon accessing this page, the user's primary TOL MTF will be displayed. The user will have the option of selecting an alternate region/MTF for their prescription refill. If the Composite Health Care System (CHCS) host participates in the TRICARE Mail Order Pharmacy (TMOP) refills program, "Mail Order" will be a selectable "Pick Up" location. Required information on the page for a prescription status request is:

- Last four digits of the Sponsor's Social Security Number (SSN). This field is pre-populated with the TOL user's sponsor information. This field can be edited.
- Numeric Portion of the Prescription Number

• Desired Pick-up Location

Required information on the page for prescription refill request(s):

- Last four digits of the Sponsor's SSN
- Numeric Portion of the Prescription Number
- Desired Pick Up Location

The TOL PHR Data displays provide the ability for an authorized beneficiary(s) to view their own PHR Data as documented in the Military Health System (MHS) Electronic Health Record. The PHR Data displays are read-only and the user may download this data via the 'Blue Button' capability in a Portable Document Format (.pdf) or Text File (.txt) formatted file to their personal computer. The user requested PHR data is a view only and NOT retained by the TOL system. After the user session has ended, there is no storage of PHR data within the TOL system.

TOL is owned by TMA and managed under the Defense Health Services Systems (DHSS) Program Office: DHSS Program Office, Clinical Support Division (CSD)  
5203 Leesburg Pike  
Sky 2, Suite 1500  
Falls Church, VA 22041  
(703) 575-6500

(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. 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 Health Insurance Portability and Accountability Act (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. 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 is 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, beneficiaries register online, and then they receive a username and password to access TOL and their applicable screens and functions. 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 the site and obtain a username and password; but 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 a unique user-identification and password, prior to being granted system access. I&A safeguard serves as the mechanism for associating a specific user with the recorded audit events. The user's password proves proper identity, enabling the trusted system to perform authentication. The site or TOL Information Assurance Officer (IAO) 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, Solaris, Oracle Application Server, and Microsoft Windows Server. Each of the three functional areas captures security relevant events and stores them for review by the IAO.

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:

- Composite Health Care System (CHCS) for primary care appointing capability
- AudioCare for Prescription Refill capability
- DMDC DEERS for eligibility assessment via iAS for registration
- AHLTA Clinical Data Repository (CDR) for PHR Data (read only)
- AHLTA web services to provide access for online HRAs of HART/CHART and access to eForms (future capability)

**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.

An authorized TOL user can view, print, and download their PHI as displayed on the PHR Data through the 'Blue Button' capability to a pdf or .txt format by selection of the "Save Personal Health Data" link once authenticated into TOL by either CAC or DoD Self-Service (DS) (Level 2) logon. 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.

**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 register into the web site and will not have access to TOL services.

(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 register 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 not selected, the system will not provide the user's Electronic Data Exchange Personal Identifier (EDI\_PI) to retrieve their medical information via PHR data displays or gain access to external systems for online HRAs (HART/CHART), eForms submissions (future capability), or SM SaaS (future capability).

(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. Chapter 55, Medical and Dental Care; 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 TRICARE Online website, and enable beneficiaries to use online services to schedule and manage appointments, refill and reorder prescriptions, access approved health content, manage their own healthcare, and obtain accurate TRICARE information on services and benefits, claims, enrollment, and TRICARE pharmacy services.

**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 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. If you choose not to provide your information, no penalty may be imposed, but absence of the requested information will result in your not being able to access and use services and benefits through the website.

A Privacy Act Warning and Security of Information are provided electronically on the TOL website. Individuals are notified through the use of a disclaimer that TOL users see and have to acknowledge before logging into the system. Individuals are informed that the PII provided during registration is compared with PII maintained by the Defence Manpower Data Center (DMDC).

**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.**