



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Healthcare Continuing Education and Training Enterprise Subscription Service  
(Swank Healthcare)

US Army Medical Command - Defense Health Program (DHP) Funded Application

### **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. 3013, Secretary of the Army; Department of Defense Instruction 1000.30, "Reduction of Social Security Number (SSN) Use Within DoD," August 1, 2012; Army Regulation 25-1, Army Information Technology; Army Regulation 351-3, Professional Education and Training Programs of the Army Medical Department; DA PAM 25-1-1 Army Information Technology Implementation Instructions; 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 US Army Medical Department (AMEDD) Center and School has a contract with Swank Healthcare to provide an online distributed learning service for delivering and tracking Continuing Education (CE) and Continuing Medical Education (CME) training and to provide access to other hosted training materials. This service is provided to personnel assigned to DoD organizations world-wide. The online training includes medical and ancillary service courses encompassing multiple healthcare disciplines; a suite of courses meeting all mandatory training requirements recommended by The Joint Commission (TJC), Occupational Safety and Health Administration (OSHA), and/or other regulatory and accrediting bodies; site specific and specialty portals for hosting government content, accreditation of government developed content; and the associated support services as an enterprise AMEDD license. The site licenses include all DoD personnel assigned to the site regardless of service affiliation, deployment status, or employment status. This includes all active duty armed forces personnel (Army, Air Force, Marines, Navy, and Coast Guard), DoD civilians, contractors, students, volunteers, and National Guard and Reserve personnel serving on Title 10 orders affiliated or employed with the sites on full-time, part-time, student, or volunteer status. It also includes all active duty personnel holding medical occupations or skills (Military Occupational Specialty (MOS); Area of Concentration (AOC); Additional Skill Identifier (ASI)) serving in other Army Commands external to the US Army Medical Command (MEDCOM), including but not limited to the US Army Forces Command (FORSCOM), or the US Army Training and Doctrine Command (TRADOC).

The PII in the system is collected, stored, and transmitted by the contractor, Swank Healthcare. The contractor provides select electronic records and reports to the sites utilizing this service. Government site coordinators can generate facility training completion reports which include Name, Truncated SSN, discipline, assigned learning groups, and email.

The types of PII collected by this system includes name; social security number and/or DoD ID; Date of Birth; work location and e-mail address; medical discipline; and medical licensing information.

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

All systems and environments have threats that seek to exploit and cause harm to the information. Some threats are natural, some are inherent in the system design, some can be attributed to unauthorized personnel, and some to authorized personnel who make mistakes. Four general categories of threats exist: human-intentional, human-unintentional, structural, and natural. The types of privacy risks include unauthorized access or unauthorized disclosure of PII. Swank Healthcare and the government sites have applied the appropriate administrative, technical, physical security safeguards to mitigate these privacy risks as indicated in Section 3d below. The contractor will, at a minimum, apply security controls as described in National Institute of Standards and Technology Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations." Appropriate technical, personnel, physical and operational safeguards are in place for the access, collection, use and protection of information. Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal.

**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.

Authorized personnel within the US Army Medical Department Center and School, the Department of the Army Surgeon General's Medical Education Directorate who has oversight over the Medical Operational Data System (MODS); and the the Combined Arms Center, Training Management

Directorate for Digital Training Management System (DTMS).

**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.

The Swank Healthcare Privacy Policy is prominently displayed on its registration/log-in page for individuals to review. The minimum PII elements required to register for an account are name, email, and user created user ID. If individuals do not provide these PII elements, they will not be able to use this training subscription service.

(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.

The Swank Healthcare Privacy Policy is prominently displayed on its registration/log-in page for individuals to review. If individuals object to the uses of their PII and do not provide the minimum PII elements for account registration, they will not be able to use this training subscription service.

(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.

Swank Healthcare Privacy Policy.  
The Swank Healthcare Privacy Policy is based on their primary Accrediting agency's (Texas Tech) credentialing and licensure requirements as demonstrated by consistent reference to Texas Tech, Texas Tech University Health Science Center (TTUHSC), or Health.edu throughout.

Section 1: Introduction  
Health.edu, a department of Texas Tech University Health Science Center (TTUHSC), follows TTUHSC Information Technology (IT) policies regarding responsible use of computer resources for the protection of users at <http://www.ttuhs.edu/IT/policy/> and the TTUHSC general privacy policy at <http://www.ttuhs.edu/tac/privacy.aspx>.

The following privacy policy is in addition to the above-referenced policies and guidelines. Health.edu recognizes that your privacy and the protection of your personal information is important to you. We have created this privacy policy in order to demonstrate our commitment to privacy. This policy explains the type of information which is gathered and tracked, how the information is used, and with whom the information is shared. This policy applies to all information collected by or submitted to Health.edu.

Section 2: Information Collected  
Regarding visitors to our web site:  
We collect aggregate information on what pages are visited in order to assess and improve the

content of our site.

Our Web server does not automatically recognize information regarding individual users, e.g., domain name or email address.

We do not set any "cookies" to track visitor's identification or use of the site.

We disclose information that we in good faith believe is appropriate to cooperate in investigations of fraud or other illegal activity, or to conduct investigations of violations of institutional policies.

We disclose information when required or authorized by applicable law.

Registered users of Health.edu Continuing Education activities:

As a provider of online educational services, we electronically collect certain information required by certifying authorities, accrediting bodies, licensing boards or governmental agencies. We store this information on our servers. In the online medium, detailed affirmation of a users' identity and their actions while using Health.edu is necessary to verify the legitimacy of course participants.

The Health.edu system utilizes industry standard security measures to protect against the loss, misuse, and alteration of information under its control. While there is no such thing as absolute security on the Internet, we will take reasonable and prudent steps to promote the security of the personally identifiable information which you provide.

Before registering for Continuing Education activities, you will be asked to authorize disclosure of your information to third parties who assist TTUHSC in delivery and support of Continuing Education activities, such as; Accrediting Agencies, Medical Licensing Agencies, after-hours call centers, and your employer (in instances in which you wish to participate in a Continuing Education activity as a part of assigned work responsibilities by your employer).

We do not share our registrant's information with third parties, except as described herein, when allowed or required by applicable law, or with your permission.

We ask participants to complete a knowledge test as part of a continuing education activity in order to provide feedback concerning the participant's understanding of the content.

We ask participants to evaluate continuing education activities in order to improve these activities and future ones.

Participant Email addresses are collected to provide password reminders and other correspondence necessary for fulfilling customer requests. If you want to change your status at a later time, you can opt-out of email notifications on the registration page for Internet courses or you can contact us to change it. (See contact information below.)

Other Uses or Disclosures of Information:

We may use the information you provide to contact you:

To check on potential verification problems, e.g., duplicate registration for the same activity.

To ask for more detail about information you have provided, e.g., on your suggestions for improvements.

To inform you that additional continuing education activities are now available at our site, if you requested this notification.

You may request that we provide you with a copy of our record of the information that you provided to us. (See "Section 9: How to Contact Us" below.)

TTUHSC is the sole owner of the information collected on this web site.

Section 3: Links:

The Health.edu web site may contain links to web sites controlled or offered by third parties (non-TTUHSC individuals and organizations). TTUHSC hereby disclaims liability for any information, materials, products or services posted or offered at any of the third party sites linked to this web site. By creating a link to a third party web site, TTUHSC does not endorse or recommend any products or services offered or information contained at that web site, nor is TTUHSC liable for any failure or products or services offered or advertised at those sites. Such third party may have a privacy policy different from that of TTUHSC and the third party web site may provide less security than TTUHSC sites.

Section 4: Changes to the Privacy Policy:

This privacy policy is effective March 30, 2010 and applies solely to information collected by Health.

edu. If we decide to change our privacy policy, we will post those changes on our web site and modify our uses and disclosures according to the new changes for only data collected or transmitted at the time of the policy change forward. Please periodically check this privacy policy for changes.

**Section 5: Availability**

Health.edu Continuing Education activities are not intended for distribution to, or use by, any person or entity in any jurisdiction or country where such distribution or use would be contrary to local law or regulation.

**Section 6: Additional Terms**

Certain sections or pages on the Health.edu web site may contain separate terms and conditions, which are in addition to these terms and conditions. In the event of a conflict, the additional terms and conditions will govern for those sections or pages.

**Section 7: Additional Terms**

Certain sections or pages on the Health.edu web site may contain separate terms and conditions, which are in addition to these terms and conditions. In the event of a conflict, the additional terms and conditions will govern for those sections or pages.

**Section 8: Governing Law**

This policy and use of Health.edu Continuing Education Activities shall be governed by and construed in accordance with the laws of the State of Texas. If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from the other provisions and shall not affect the validity of the other provisions.

**Section 9: How to Contact Us**

If you have any questions or concerns about this privacy policy or this web site, you may contact:  
health.eduhelpdesk@ttuhsc.edu

**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.**