Privacy Impact Assessment for the VA IT System called:

Train Learning Management System - Enterprise (Train-E)

Veteran's Health Administration (VHA)

Institute for Learning, Education and Development (ILEAD)

Date PIA submitted for review:

08/21/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.Katz-Johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Randall Smith	Randall.Smith@va.gov	319-338-0581x636266
Information System Owner	Aimee Barton	Aimee.Barton@va.gov	216-707-7726

Abstract

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

TRAIN is a Learning Management System created by the Public Health Foundation in order to make educational content from various government entities available to a wide range of public users. Anyone can access the content on TRAIN; it lets the learner save the courses they want to take and keeps up with their completion. VA content that is available on TRAIN is served from an Akamai content server that is part of the TRAIN subscription. This entry is for an administrative ATO for the system that is in production while Project Special Forces works on the FedRAMP and Internal ATO's

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

Train Learning Management System – Enterprise, Institute for Learning, Education and Development (ILEAD)

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.

TRAIN is a Learning Management System created by the Public Health Foundation in order to make educational content from various government entities available to a wide range of public users. Anyone can access the content on TRAIN; it lets the learner save the courses they want to take and keeps up with their completion. VA content that is available on TRAIN is served from an Akamai content server that is part of the TRAIN subscription. This entry is for an administrative ATO for the system that is in production while Project Special Forces works on the FedRAMP and Internal ATO's.

C. Indicate the ownership or control of the IT system or project.

VA Controlled / non-VA Owned and Operated

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

Approximately 1000

E. A general description of the information in the IT system and the purpose for collecting this information.

TRAIN Learning Network (TLN) is a Learning Management System (LMS) that manages and tracks TLN user training activities. TLN administrators use the system to create and manage

training content records that can be included in a larger training content catalog for broad TLN user access.

F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.

Data is not shared.

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.

Does not use multiple databases.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

OPM-GOVT 1 – OPM_GOVT: AUTHORITY FOR MAINTENANCE OF THE SYSTEM INCLUDES THE FOLLOWING WITH ANY REVISIONS OR AMENDMENTS: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, 9830, and 12107

76VA05- General Personnel Records (Title 38) AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501(a), 7304, 7406(c)(1), and 7802.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

The owner has been made aware that the SORN is from 2000 and these questions cannot be answered until the revision is published.

D. System Changes

J. Whether the completion of this PIA will result in circumstances that require changes to business processes

No

K. Whether the completion of this PIA could potentially result in technology changes

No

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☐ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Gender
- ☐ Integrated Control Number (ICN)
- ☐Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Organization, Job Title/ Role, Professional License Number, Education Level, Primary/Secondary Language, FEMA Student ID Number, Professional Organization ID Number

PII Mapping of Components (Servers/Database)

Train Learning Management System – Enterprise (Train-E) consists of <**number**> key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Train-E** and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
SQL Server	**Yes**	**Yes**	•Name • Phone Number • Address • Organization • Job Title / Role • Professional License Number • Education Level • Gender • Ethnicity • Race • Birth Date • Primary/Secondary Language • FEMA Student ID Number • Professional Organization ID Number	User identification and course assignment targeting	MFA VPN required for admin access; Private, internal network; least privilege access; SQL audit logging; credentialed vulnerability scanning.

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.
Organization provided user data, self-provided user data
1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Data is collected directly from the individual, or it is provided by the user's organization (i.e. VHA)

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

The organization administering the system may wish to create accounts for their end-users in a bulk, batch process.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

The system creates information based on online training test scores and analytic reports.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Information is collected directly in a user's web browser.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

Not subject to the Paperwork Reduction Act

1.4 How will the information be checked for accuracy? How often will it be checked?

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

No information accuracy checks are in place.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

Does not use commercial aggregator of information

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

Please provide response here

OPM-GOVT 1 – OPM_GOVT: AUTHORITY FOR MAINTENANCE OF THE SYSTEM INCLUDES THE FOLLOWING WITH ANY REVISIONS OR AMENDMENTS: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, 9830, and 12107

76VA05- General Personnel Records (Title 38) AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501(a), 7304, 7406(c)(1), and 7802.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

<u>Principle of Purpose Specification:</u> Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

<u>Principle of Minimization:</u> Is the information directly relevant and necessary to accomplish the specific purposes of the program?

<u>Principle of Individual Participation:</u> Does the program, to the extent possible and practical, collect information directly from the individual?

<u>Principle of Data Quality and Integrity:</u> Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: There is a risk of employee PII could be accessed by unauthorized person.

Mitigation: Only individual employees/contractors/trainees have access to their information. Only few authorized individuals have access to all system information. Home - VHA TRAIN - an affiliate of the TRAIN Learning Network powered by the Public Health Foundation

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

System provides training to providers; information in the system is used to track training.

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

This system does not analyze any data.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

Learning and training progress records are created and associated with existing user records based on online training activities. This information is available to VHA TRAIN administrators for tracking and administrative purposes.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

In addition to FedRAMP Low Baseline security controls, PII is secured in the system through various administrative, technical, and physical measures. Highlighted below is a brief selection of key controls.

Administrative: System and data access is delegated by following the principles of least privileged access–only the minimum access needed for a role or function is granted. Access is granted only after receiving management approval for the specific access.

Technical: All systems within the boundary have automation-driven, host-based firewalls that allow only necessary traffic. Remote administrative access to systems is only available via MFA VPN connections. Role-based access controls segregate user bases within TRAIN's shared environment.

Physical: The system runs on a private cloud infrastructure residing within an ISO 27001-certified facility. Independent third-party assessments for SOC 1, SOC 2,
HIPAA and PCI-DSS are performed annually. Key cards, biometrics, and physical keys are required to access the data center floor.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

*T*he system *does n*ot collect, process, or retain Social Security Numbers,

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

In addition to FedRAMP Low Baseline security controls, PII is secured in the system through various administrative, technical, and physical measures. Highlighted below is a brief selection of key controls.

Administrative: System and data access is delegated by following the principles of least privileged access–only the minimum access needed for a role or function is granted. Access is granted only after receiving management approval for the specific access.

Technical: All systems within the boundary have automation-driven, host-based firewalls that allow only necessary traffic. Remote administrative access to systems is only available via MFA VPN connections. Role-based access controls segregate user bases within TRAIN's shared environment.

Physical: The system runs on a private cloud infrastructure residing within an ISO 27001-certified facility. Independent third-party assessments for SOC 1, SOC 2,
HIPAA and PCI-DSS are performed annually. Key cards, biometrics, and physical keys are required to access the data center floor.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. ***Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.***

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

Through reports on who has completed training

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

No

2.4c Does access require manager approval?

Yes

2.4d Is access to the PII being monitored, tracked, or recorded?

Yes. logs on who accessed reports are available

2.4e Who is responsible for assuring safeguards for the PII?

Administrators,

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

TRAIN system logs are retained for 1 year. TRAIN user training data is retained indefinitely.

3.2 How long is information retained?

*In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. **For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods**. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

TRAIN system logs are retained for 1 year. VA Records Control Schedule 10-1 Temporary. Redirects as referenced in National Archives and Records Administration (NARA) Disposition Authority DAA-GRS-2013-0006-0003, item 030. Temporary. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system. Destroy when business use ceases. https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes

3.3b Please indicate each records retention schedule, series, and disposition authority.

National Archives and Records Administration (NARA) Disposition Authority DAA-GRS-2013-0006-0003, item 030. Temporary. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system. Destroy when business use ceases.
https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.
https://www.va.gov/vapubs/search_action.cfm?dType=1

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

Any PII used for testing purposes is fully anonymized.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: There is a risk that information could be maintained longer than necessary.

Mitigation: Only the minimum necessary information is retained. TRAIN system logs are deleted after 1 year. VA Records Control Schedule 10-1 Temporary. Redirects as referenced in National Archives and Records Administration (NARA) Disposition Authority DAA-GRS-2013-0006-0003, item 030. Temporary. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system. Destroy when business use ceases.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
N/A	N/A	N/A	N/A

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk:

Mitigation :

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk:

Mitigation:

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not? Yes

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Notice is provided at time of account creation in the form of system use policies. Users must confirm "I agree to all TRAIN policies" to create an account.

The following VA System of Record Notices (SORNs) which are published in the Federal Register and available online

OPM-GOVT 1 – OPM_GOVT

76VA05- General Personnel Records (Title 38)V

This Privacy Impact Assessment (PIA) also serves as notice As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Please provide response here

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

Notice is attached in Appendix A 6.1

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Yes, individuals can decline but it will forfeit the ability to use TRAIN.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

There are no specific options for partial consent, only full consent is allowed for system use.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: There is a risk that individuals will be unaware that their information is being collected.

Mitigation: All individuals are given a notice in the prior to participate in the training which they have to accept in order to access training. During initial log in the user agrees to TRAIN policies, that the user is agreeing to log into a Federal Government sponsored system as well as govDelivery Subscriber Cookie Statement. VA Privacy Notice Home - Privacy, govDelivery Subscriber Cookie Statement (granicus.com)

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.
A user is able to view their account information and amend as needed. Course records are available typically in the form of completion certificates. Course records cannot be changed.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Support is provided by VHA and posted on TRAIN as follows: "If you require assistance, please contact the VHA TRAIN Help Desk by email at VHATRAIN@va.gov."

The information is contained in SORNS OPM-GOVT 1 – OPM_GOVT
76VA05- General Personnel Records (Title 38)V

Which describes the process for access

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

This system is not exempt from the access provisions of the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

The VHA TRAIN Help Desk (VHATRAIN@va.gov) is able to correct inaccurate or erroneous information.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The correction procedures are the same as those given in question 7.1 .

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

A Support link is available on the TRAIN website that direct VHA users to their appropriate contact group: https://www.train.org/vha/contacts

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

A Support link is available on the TRAIN website that direct VHA users to their appropriate contact group: https://www.train.org/vha/contacts

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk that individuals will not know how to correct inaccurate/erroneous information.

Mitigation: *A Support link is available on the TRAIN website that direct VHA users to their appropriate contact group: https://www.train.org/vha/contacts, to fix any inaccuracies.* Home - VHA TRAIN - an affiliate of the TRAIN Learning Network powered by the Public Health Foundation

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

Only administrators receive access to the system; permission is granted by an existing administrator.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Users of other government agencies do not have access to the system information.

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Only a handful of individuals have access to the reports run by administrators; all reports are read only

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system? No

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes. CSP could have access to employee name and telephone numbers that are listed. In accordance with contract requirements with Train they are required to take privacy and information security training VA10176 before being granted access to VA information. Train is required to provide the Contracting Officers Representative with a copy of the completed certificate.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

All VA employees are responsible for taking VA10176 Information Security and Rules of Behavior training. Individuals who have access to protected health information are also required to take Privacy and HIPAA training VA10203

8.4 Has Authorization and Accreditation (A&A) been completed for the system? Yes

8.4a If Yes, provide:

1. *The Security Plan Status: Active*
2. *The System Security Plan Status Date: 26-Nov-2021*
3. *The Authorization Status: Authority to Operate*
4. *The Authorization Date: 08-Jul-2021*
5. *The Authorization Termination Date: 07-Jul-2024*
6. *The Risk Review Completion Date: 06-July-2021*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH): Low*

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

N/A

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Yes, it is a FedRAMP approved SaaS product. FedRAMP Package ID FR2113157410. Private Service Provider: Cologix Columbus Data Center.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

VA owns rights over data.

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

No

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

ILEAD has contracted DTS to provide external LMS; both ILEAD, Contractor and TRAIN manage risks.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2023.09.28 14:23:20 -04'00'

Privacy Officer, Nancy Katz-Johnson

RANDALL SMITH

Digitally signed by RANDALL SMITH
Date: 2023.09.28 13:37:00 -05'00'

Information Systems Security Officer, Randall Smith

AIMEE BARTON

Digitally signed by AIMEE BARTON
Date: 2023.10.23 16:01:27 -04'00'

Information Systems Owner, Aimee Barton

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

I. General Policies and Liability Terms

www.Train.org is owned and operated by the Public Health Foundation (PHF) with assistance from the TRAIN Learning Network (TRAIN) Affiliates. Neither PHF nor the TRAIN Affiliates receive commissions or any other financial compensation related to user enrollment in a course or purchase through this system, unless a course is specifically noted as being offered by PHF or an Affiliate organization for a fee.

All registrations, purchases, obligations, and course communications are the responsibilities of users and providers. Neither PHF nor Affiliates will arbitrate disputes.

Because www.Train.org and TRAIN Affiliates rely on submission of data by the participating users, PHF and Affiliates are not responsible for errors, omissions, or timeliness in any data submitted, including courses, documents, announcements, and other materials submitted on the www.Train.org and TRAIN sites by any person. PHF is not responsible for erroneous, defamatory, or illegal information submitted to www.Train.org and TRAIN, nor for any damages that may be suffered as a consequence of these posting.

Unless noted otherwise, neither PHF, its agents, nor TRAIN funding partners, sponsors, or Affiliates are responsible for course content or the accuracy of listing information, which is entirely the responsibility of course providers.

PHF is the owner of all data entered and managed through the national www.Train.org site. TRAIN Affiliates have access to review course data on www.Train.org for assessment and planning purposes, but have no authority to sell or otherwise transfer any information from the national www.Train.org site or any data from another Affiliate to any person(s) without the prior written consent of PHF.

Data from www.Train.org or any TRAIN Affiliate site may not be sold. This prohibition covers all course listings, providers, learners, and any other site data.

PHF reserves the rights, which may be exercised in PHF's sole discretion, to (a) edit Affiliate-approved course listings for clarity and overall consistency within www.Train.org and TRAIN submission requirements; (b) refuse or revoke any organization's privilege to list any course if it is inconsistent with the purpose, scope, and target audiences of www.Train.org and TRAIN, or for any other reason; or (c) delete duplicate or inappropriate records.

PHF will not use Affiliate learner record data or Affiliate-approved course provider data for PHF communications or marketing unless written permission is given or individuals request to receive information about new courses or other site news through the "Save this Search" and other notification features on www.Train.org or TRAIN sites.

The goods and services provided within the www.Train.org and TRAIN network are provided without any express or implied warranties of (a) merchantability, or (b) fitness for a particular purpose. PHF shall not be liable to any Affiliate or third party for any loss of profits, loss of use, interruption of business, or any direct, indirect, incidental or consequential damages of any kind arising under or in connection with www.Train.org or TRAIN.

Access delays, errors or unavailability of the site may occur due to modification or maintenance of www.Train.org and TRAIN sites or for other reasons which may be beyond PHF's control. PHF is not liable to Affiliates, course providers, or users for any such delays, inconvenience or unavailability of site(s), regardless of cause.

Links to and from www.Train.org and TRAIN Affiliates do not constitute an endorsement by PHF or Affiliates of the parties or their products and services. PHF and Affiliates are not responsible for the accuracy or content of information contained in the links to third party sites. The confidentiality statements of PHF and Affiliates do not extend to any third party sites.

PHF and Affiliates may compile and publish commentaries and reviews regarding any of the courses, features and materials listed on TRAIN or www.Train.org .

PHF is committed to processing data in accordance with our responsibilities under the GDPR. Article 5 of the GDPR requires that personal data shall be:

processed lawfully, fairly and in a transparent manner in relation to individuals;

collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safe guard the rights and freedoms of individuals; and

processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

II. Confidentiality Statement

TRAIN Affiliates have access to all learner records, including transcripts, entered and managed through their Affiliate site and have the right to delete or edit all such learner records. Affiliates may use individual or aggregate data from learner records for any public health purpose, including but not limited to workforce assessments, performance management, federal grant reporting, and communications related to public health preparedness training and emergency responses requiring trained personnel. Affiliates may further restrict the use of learner record data in accordance with the policies and laws governing the Affiliate site and organization.

Affiliates may assign rights to access learner records to local public health agencies or other entities responsible for public health workforce training, and the Affiliate shall assure that the agency or entity abides by the privacy and confidentiality commitments contained herein. Affiliates may grant access rights to learner records to vendors performing evaluation or other duties on the Affiliate's behalf, so long as such vendors agree to the confidentiality terms set forth by PHF.

PHF will not alter or delete learner records from an Affiliate site except to transfer a record to another Affiliate, make necessary repairs, or as otherwise requested by the learner or Affiliate that has rights to the record.

When a learner chooses to register for a course through www.Train.org or TRAIN, the course provider may access required and optional contact information contained in the learner record for communications related to the course. Course providers have no access to transcript information in the learner record.

PHF and its vendors have access to all learner records in TRAIN. PHF and any vendors used by PHF, Affiliates, or their designees agree that learner records containing transcripts and individually identifying data will not be disclosed to any third party, except upon the written authorization of the learner, or upon the order of a court of competent jurisdiction.

Records received or created as part of the official business of the Florida Department of Health are subject to Florida's public records laws and will be provided in response to a public records request unless exempt and/or confidential under Florida law.

After excluding any individually identifying data, PHF and Affiliates may compile and aggregate data from Affiliate learner records for analysis, assessments, and planning purposes to a third party.

Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data, we shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach

III. Learner Rights and Responsibilities

Your Affiliate site's administrator(s), PHF and its vendors or designees that agree to www.Train.org and TRAIN confidentiality policies may access learner records, including transcripts.

Identifiable information in your learner record will not be disclosed to any third party, except:

With your written authorization.

Upon the order of a court of competent jurisdiction.

If you choose to register for a course through www.Train.org or TRAIN. Registration enables the course provider to access the contact information that you provide for communications related to the provider's course. Course providers have no access to transcript information in the learner record.

Records of Florida Department of Health employees are not subject to paragraphs a. and b., supra. Records of Florida Department of Health employees are subject to Florida's public records laws at Chapters 119 and 286, Florida Statutes, and Art. I, Sec. 24, Florida Constitution.

It is your responsibility to keep your learner record up to date, and you have the right to update your learner information at any time.

Should you desire your record to be transferred to another Affiliate or to a third party, contact your site administrator for more information on this process. In most cases, changing your address will automatically transfer your record to the appropriate TRAIN Affiliate site, if available. As new states and organizations join TRAIN, PHF will transfer the management of

records as appropriate to the Affiliate's jurisdiction. If needed, PHF will transfer your learner records to another Affiliate or to a third party with your written permission.

For TRAIN learners under the GDPR, you have the right to have your learner record removed from TRAIN. To do so contact your site administrator for more information.

Your individual learner data will not be used by PHF for marketing any products or services without your prior written consent. Affiliates may use your contact information to reach you in the event of an emergency or to alert you to important public health information and training. If no Affiliate exists in your public health jurisdiction, and your record is on the national TRAIN site, PHF may use your contact information for the same purposes.

PHF will exclude any individually identifying data before compiling or publishing data about the health workforce that draws from your learner record. Individually identifying data includes your first name, middle name, last name, street address, email, telephone, mobile, fax, pager, or equivalent fields.

All fees and expenses for any course are to be handled between you and the course provider. PHF and Affiliates are not responsible for registration or fees and expenses related to any third-party course. Neither PHF nor Affiliates will arbitrate disputes.

Neither PHF nor any of its funding partners, Affiliates, or sponsors are responsible for the endorsement of courses, nor for course content, which is entirely the responsibility of the course providers. We encourage you to carefully review all course descriptions and contact the course provider or developer in making your own decisions about the quality and suitability of courses for your learning needs.

www.Train.org and TRAIN may offer links to other websites. The confidentiality commitment of PHF for its site does not extend to any third party sites. We encourage you to review the policies of all third party sites that may be linked from www.Train.org and TRAIN.

Affiliates may further restrict the use of learner record data in accordance with the policies and laws governing the Affiliate site and organization.

Terms of Use:

PHF reserves the right to change, at any time, these terms and conditions, and the information contained herein.

If you feel that PHF or an Affiliate has violated this Confidentiality Statement in any way, please contact PHF at training@phf.org so we may address the issue.

By registering as a user on any www.Train.org or TRAIN Affiliate site, you acknowledge that you have read, understood, and accepted PHF's General Policies and Liability Terms, Confidentiality Statement, and Learner Rights and Responsibilities.

IV. Course Provider Rights and Responsibilities

Course Providers are responsible for entering their course information into the www.Train.org database and keeping this information up to date.

As a Course Provider, you agree to allow the Public Health Foundation (PHF) and TRAIN Learning Network (TRAIN) Affiliates use of your course titles and organizational name for publicity of the www.Train.org or TRAIN Affiliate sites.

All approved Course Providers will be opted-in to receive emails from TRAIN in order to allow TRAIN Administrators to communicate with them about their course listings. Once approved, you will not be able to opt-out of receiving TRAIN emails without also losing your Course Provider access.

All courses entered by approved organizations will be placed in a temporary holding bin until approved for listing by the site administrator(s). Course Providers will be notified by e-mail upon approval or denial of a course. Furthermore, courses will automatically become de-activated once the entered deactivation date arrives. As a Course Provider, you may modify the date prior to de-activation.

PHF and Affiliate administrators reserve the right to edit your course listings, subject areas, target audiences, or other attributes for clarity and overall consistency with www.Train.org submission requirements. TRAIN Affiliates also reserve the right to block any course from view on their individual site, even if the course was approved by another TRAIN Affiliate.

PHF reserves the right to refuse or revoke any organization's privilege to submit courses to www.Train.org that are inconsistent with the purpose, scope, and target audiences of www.Train.org, or for any reason.

Course Providers should list their courses on TRAIN through only one TRAIN site. Each Course Provider must choose to use either the national www.Train.org site or one of the TRAIN Affiliate sites based on the guidance below. The site selected does not affect the visibility of courses to users throughout TRAIN. It affects the site administrator that manages your registration and course listings.

Course Providers Primarily Serving a TRAIN Affiliate Jurisdiction

Course providers that primarily serve an Affiliate's jurisdiction should register to list their courses through the respective TRAIN Affiliate site.

"Primarily serving the Affiliate's jurisdiction" means that most of the provider's public health courses are designed for and restricted to the workforce of the jurisdiction covered by the Affiliate.

Course providers that also offer courses designed for a national or regional audience can be entered and approved through the same Affiliate site, so long as these courses comprise a minority of course offerings. Once approved, nationally available courses will be visible to all learners on www.Train.org.

Course Providers Primarily Serving a National, International, or Regional Audience:

Course providers that primarily serve a national, international (including the United States), or regional audience comprised of two or more states should register to list their courses through the national www.Train.org site.

Regional course providers must designate on the course listing each state or jurisdiction that is eligible to participate. Once the course is approved for listing by PHF, the regional course information will be visible to learners from the corresponding jurisdictions.

National and international course providers should enter their course information through the national TRAIN site. Once approved, nationally available courses will be visible to all learners on www.Train.org.

Course Providers Serving Non-Affiliate Jurisdictions:

Courses that are designed for and restricted to the workforce of Non-Affiliate jurisdictions are not eligible to be listed on www.Train.org.

Course providers that primarily serve non-Affiliate jurisdictions may register to list courses on www.Train.org that serve a national, international, or regional audience and meet other submission requirements.

Terms of Use:

PHF reserves the right to change, at any time, these terms and conditions, and the information contained herein.

If you feel that PHF or an Affiliate has violated this Confidentiality Statement in any way, please contact PHF at training@phf.org so we may address the issue.

By registering as a course provider at any TRAIN Affiliate site or www.Train.org , you acknowledge that you have read, understood, and accepted PHF's General Policies and Liability Terms, Confidentiality Statement, Learner Rights and Responsibilities, and Course Provider Rights and Responsibilities.

V. Definitions

Administrator

Any designated person that manages and approves course providers, learners, courses, or other items on www.Train.org or a TRAIN site.

Affiliate

Any organization - such as a state public health agency, regional training center, or professional association - that purchases and is responsible for managing a customized website that is part of the TRAIN Learning Network (TRAIN).

Affiliate jurisdiction

The state, locality, or other geographic area or constituency served by an Affiliate as established by statute, bylaws, or other authority.

Course provider

Any public or private organization that delivers training and registers to submit their organization's training programs on national or Affiliate TRAIN site. The course provider and its courses are subject to administrator approval.

Individually identifying data

Includes the following required and optional fields in the learner records: first name, middle name, last name, street address, email, telephone, mobile, fax, pager, or equivalent fields.

Learner

Any public health or health professional that uses national or Affiliate TRAIN sites to find, register for, or track his or her participation in training opportunities.

Learner record

An individual's electronic record within TRAIN containing entered contact information, other individual attributes, and a transcript of his or her participation in training programs either automatically tracked by the system or entered by the learner.

Non-Affiliate

Any state or other organization that has not purchased a customized website that is part of the TRAIN Learning Network (TRAIN).

Site

A term used to describe the national www.Train.org and TRAIN website(s).

Site administrator

See term Administrator.

TRAIN

The TRAIN Learning Network is a web based nationwide learning management system for public health organizations that are affiliated with www.Train.org.

www.Train.org

The Public Health Foundation's (PHF) online learning clearinghouse where the public health workforce can search the extensive database of nationwide and international courses, submit courses, and track learning. User. Any Affiliate, Learner, Course Provider, or other person that views, enters, or manages information on www.Train.org and TRAIN sites.

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices