Privacy Impact Assessment for the VA IT System called:

Salesforce: Educational Activity Records (EARs) Automation

VHA

Discovery, Education, and Affiliate Networks (DEAN)

Date PIA submitted for review:

8/22/2023

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)	James Boring	*James.Boring@va.gov*	*215-842- 2000, Ext: 4613*
Information System Owner	*Mike Domanski*	michael.domanski@va.gov	727-595-7291

Abstract

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

Salesforce: Educational Activity Records (EARs) Automation is meant to replace the health professions trainee (HPT) educational activity tracking and reimbursement accounting at VA which is currently accomplished utilizing Excel spreadsheets. EARs Automation is a web-based tool needed to improve accuracy, reduce errors, produce reporting, increase accountability and to respond to government accountability office (GAO).

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.

Salesforce: Educational Activity Records (EARs) Automation and Discovery, Education, and Affiliate Networks (DEAN)

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

It is a tracking tool meant to help improve and replace the current manual process of tracking HPTs educational activities and reimbursements.

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

Salesforce owns this application as it is being built in the environment and the control is through the Discovery, Education, and Affiliate Networks (DEAN) office.

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.

The database stores VA educational activity and reimbursement information for approximately 50,000HPTs annually participating in post-graduate training programs.

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

HPT profile, VA educational activity and reimbursement at 150 VA facilities is currently tracked and recorded on Excel spreadsheets. An automated, web-based tool is needed to improve accuracy, reduce errors, produce reporting, increase accountability and to respond to GAO.

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

No data will be shared with or by this system

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.*

The system will be used by approximately 150 VA facilities. Data and controls will be standardized across sites.

3. Legal Authority and SORN

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

Although ***Salesforce: Educational Activity Records (EARs) Automation*** data is stored in the Salesforce FedRAMP cloud, it remains the property of the VA and as such, the VA remains responsible for the security and privacy of this data. The VA enforces these protection requirements through the implementation of its cybersecurity policies and the Risk Management Framework (RMF) process. Under the RMF Process, the system has a Data Security Categorization of ***Moderate***, with the impacts of a data compromise being identified in the ***Salesforce: Educational Activity Records (EARs) Automation*** Data Security Categorization (DSC) memo. The Privacy Act is the legal authority to utilize this information.

The Privacy Act is the legal authority to utilize this information. The Privacy Act of 1974, set forth at 5 U.S.C. 552a, states the legal authority to utilize this information. As per the SORN, The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12.

The system is covered by SORN 76VA05 SYSTEM NAME: Altered System of Records, General Personnel Records (Title 38)–VA.. The 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?*

Salesforce: Educational Activity Records (EARs) Automation will not

- Cause any technology changes, nor
- Affect the relevant SORN applicable for the system is 00-18287.pdf (govinfo.gov) System Name: Privacy Act of 1974, Altered System of Records, General Personnel Records (Title 38)—VA 76V The SORN covers all Personally Identifiable Information (PII) used in ***Salesforce: Educational Activity Records (EARs) Automation***

D. System Changes

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

Salesforce: Educational Activity Records (EARs) Automation will not cause any business processes to change.

K. Whether the completion of this PIA could potentially result in technology changes
Salesforce: Educational Activity Records (EARs) Automation will not cause any technology changes

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)

*Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

- HPT's Training program name
- HPT's Training level
- HPT's (financial information) Daily rate (based on salary and benefits)
- HPT's Health Insurance type (only type but no specifics e.g., self, self plus one, family)
- HPT's citizenship status
- HPT VISA status

PII Mapping of Components (Servers/Database)

Salesforce: Educational Activity Records (EARs) Automation consists of 0 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 Salesforce: Educational Activity Records (EARs) Automation 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
N/A					

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.

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 from academic affiliates who hire the health professions trainees (HPTs) and schedule their clinical training program.

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.

. Data for each HPT is provided by the academic affiliate. VA reimburses the affiliate for the HPT's educational activity while on VA rotation. We do not pay the HPT directly. The HPT does not play a role in the reimbursement process to the affiliate other than perform VA rotations.

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

The automated system will produce a "Financial Summary" in which the affiliate will utilize to invoice VA for the reimbursement of the educational activity of their HPT's while on VA rotation.

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?

Data is provided to VA facilities by the academic affiliates through existing policy-based processes. Academic affiliates are required to submit the names, training programs, training level, and citizenship through the Trainee Qualifications and Credentialing Verification Letter (TQCVL) to onboard the HPTs as without compensation employees at VA facilities. The academic affiliates provide the health insurance type and training schedule for each HPT. The HPT's time and attendance will be tracked and documented via the EARs system throughout their VA rotations. The time and attendance data will be compiled, reconciled and sent to the affiliate to be utilized to invoice VA.

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.

Information is provided by the academic affiliate via email.

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.

Information about HPTs is updated annually or as needed throughout an academic year. HPT schedules are updated monthly or more frequently. Information is confirmed through updates from academic affiliates as well as internal VA without compensation appointment data.

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 apply.

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

- Title 38 U.S.C. § 7302 Functions of Veterans Health Administration: Health-Care Personnel Education and Training Programs established the authority for academic affiliations. The Veterans Health Care Expansion Act (1973) and the Title 38 U.S.C. § 7406 - Residencies and Internships (1991) authorized agreements with academic affiliates for the central administration of the salary and benefits for residents rotating at VA facilities.
38 U.S.C. § 7402 (1991) Functions of Veterans Health Administration: health-care personnel education and training program.https://www.govinfo.gov/content/pkg/USCODE-2011-title38/pdf/USCODE-2011-title38-partV-chap73-subchapI-sec7302.pdf.
Veterans Health Care Expansion Act; Public Law (P.L.) 93-82,
https://www.govinfo.gov/content/pkg/STATUTE-87/pdf/STATUTE-87-Pg179.pdf.

U.S.C. § 7402. Residencies and internships. https://www.govinfo.gov/app/details/USCODE-2015-title38/USCODE-2015-title38-partV-chap74-subchapI-sec7406.

The system is covered by SORN 76VA05 SYSTEM NAME: Altered System of Records, General Personnel Records (Title 38)–VA.. The AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501(a), 7304, 7406(c)(1), and 7802.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.
Reimbursement to academic affiliates for HPT educational activities while on rotation at VA facilities, known as disbursement, is a statutory process that has been under increased scrutiny of Congress, the Office of the Inspector General (OIG) and the General Accountability Office (GAO). The disbursement process is on the Enterprise Risk Register. To mitigate financial and reputational risk, use of VA's $850 million disbursement budget must be accurate and, therefore, requires specific HPT information including names, training program, training level, citizenship status, health insurance type, the salary and benefits applied to that training level, and their training schedules. For the purposes of audits and to address oversight requirements, HPT activity records must contain the required data in order to prevent overpayment, underpayment, fraud, waste and abuse.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?
Yes. The information collected is directly relevant and necessary to reimburse the affiliate accurately.
***<u>**EARs Automation minimizes the PII needed to accomplish the goals of the organization.**</u>

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?
No VA collects the data directly from academic affiliates who collects the information from the HPTs. Salary and benefits are set by the academic affiliate, are applied to the specific program, training level, citizenship status, health insurance type and shared directly with VA. The reimbursement relationship is between VA and the academic affiliate not VA and individual HPT.

Principle of Data Quality and Integrity: 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.

Privacy Risk: PII used in EARs Automation to track HPT educational activities while on VA rotation to assure accurate reimbursement and VA fiscal responsibility.

Mitigation: EARs Automation does not collect any other PII besides name, training program and level, citizenship status, daily rate, and health insurance plan. That information is often publicly available on training program websites. The information collected in EARs Automation is only shared with the VA facility's academic affiliate and the VA Office of Academic Affiliations.

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.

- Name: Used to identify HPTs' educational activities while on VA rotation.
- Training level: The HPT's year of post graduate level of training is used to identify the daily rate to calculate accurate reimbursement for educational activity while on VA rotation. and shared with the academic affiliate who is the primary source of this information.
- Daily rate: The daily rate is set by the affiliate, training program and training level and is used to calculate accurate reimbursement for HPT educational activity while on VA rotation.
- Health Insurance type: VA reimburses through disbursement for both salary and benefits which are set by the academic affiliate by training program and training level.
- Citizenship and VISA status: Nonresident alien students and trainees temporarily present in the United States in F-1, J-1, M-1, or Q-1 nonimmigrant status are exempt from social security and Medicare taxes on wages paid to them. This must be tracked as it will affect salary and subsequently their daily rate.
- Training Program: An academic (health professions education [HPE]) program is an organized unit of study or pattern of courses and related experiences to accomplish a specific education objective such as an academic degree, certificate, diploma, or other formal recognition. Generally, these are in health professions fields and require clinical training experiences.
- The information above is share with VA staff involved in the tracking and reimbursement of HPT educational activity while on VA rotation and with the academic affiliate who is the primary source of this information.

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.

Storing information in regard to the date and location of the HPT while on VA rotation. EARs automation will calculate the number of reimbursable days multiplied by the daily rate (daily rate = PGY level, salary, benefits, health insurance status, citizenship status) = total reimbursement to the affiliate. The reimbursement amount can be reflected by affiliate, program, HPT, daily, monthly, quarterly, or annually. Standard Salesforce tools will be used to analyze data such as reports, dashboard, and record pages.

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.

EARs Automation will create HPT educational activity reports which will then be integrated into a calculation to determine reimbursable amount to affiliates. Reports generated are for the sole purpose of tracking educational activity of HPT's while on VA rotation for reimbursement to the affiliate, auditing of such activity and reimbursements, and management of allocated funds and full-time equivalent (FTE) positions. Any action taken because of data generation will have no effect on the HPT. No data collected, generated, or stored for EARs automation will be placed in the HPTs existing records outside of EARs automation.

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?

- This system utilizes Salesforce Shield Protect which provides a FIPS 140-2 certified encryption. For data in transit between the database and users of the system, it will be secured through Salesforce shield and other standard salesforce security tools (private sharing model, permission sets, sharing rules, etc...) There is no other transit state because this system will not be integrated with any other system.

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

- No SSNs are collected, processed or retained by the system

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

- This system utilizes Salesforce Shield Protect which provides a FIPS 140-2 certified encryption.

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?

- Information will be restricted only to users who need said access via standard security controls such as field-level-security, sharing rules for record sharing and permission sets for table/object access.

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

- Yes. Will be documented in the in the solution architecture package.

2.4c Does access require manager approval?

Yes

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

- Yes

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

- Each local facility will adhere to standard PII protocol.

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*

- All data listed in 1.1 will be retained by VA facility in accordance with Department of Veterans Affairs Records Control Schedule 10-1 for 7 years after the education activity is closed..

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.*

1100.40 Educational Activity Records:1100.40a. Paper files. Hardcopy version of information manually entered into project/program files. Temporary. Destroy 7 years after the education activity is closed. If an accepted digital copy has been made, destroy immediately. 1100.40b. Electronic files. Electronic and/or digital version of information entered into project/program files. Temporary. Destroy 7 years after the education activity is closed.

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.

Yes – it is in 10-1.

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

The retention schedule for the Salesforce Development Platform (SFDP) also applied System Name/ Acronym module. SFDP complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6500. Records contained in the Salesforce FedRAMP cloud will be retained as long as the information is needed in accordance with a NARA-approved retention period. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). SFDP records are retained according to Record Control Schedule 10-1 Section 4. (Disposition of Records)

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

Records Control Schedule 10-1, Item Number 1100.40 Educational Activity Records. Paper files: (Temporary) Destroy 7-years after the education activity is closed. If an accepted digital copy has been made, destroy immediately. Electronic files: (Temporary) Destroy 7-years after the education activity is closed.

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.

Salesforce: Educational Activity Records (EARs) Automation tool adheres to the VA RC Schedule 10-1. All electronic storage media used to store, process, or access records will be disposed of in adherence with the VA Directive 6500. (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.

Only aggregate academic affiliate, program, program level and financial data will be used for research, testing or training. No PII is needed for these purposes.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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.

pull report of all records outside of the retention period and permanently delete. Probably through DTC.

Privacy Risk: HPT PII and educational activity records are held within the system.

Mitigation: All data is protected using Salesforce Shield and a FIPS-140-2 encryption. All electronic data is deleted/destroyed 7 years after the education activity is closed.

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			

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: No risk is presented as there is no internal sharing.

Mitigation: Mitigation is not needed, as no risk is presented.

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? A financial summary is sent to the affiliate so they can invoice VA. It includes the exact same information they sent us. The affiliate is the primary source of information. The financial summary could include the following: Affiliate name, Program Name, HPT name – training level – daily rate – health insurance status – citizenship Status – attendance, and reimbursable amounts.

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*	*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*	*List the method of transmission and the measures in place to secure data*

	with the specified program office or IT system		***use, etc. that permit external sharing (can be more than one)***	
Affiliate sending/receiving the information	Billing	**Affiliate name, Program Name, HPT name – training level – daily rate – health insurance status – citizenship Status – attendance, and reimbursable amounts.**	SORN - 76VA05 : Altered System of Records, General Personnel Records (Title 38)– VA	Email, VA's encryption techniques

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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:

<u>Privacy Risk:</u> Information could be sent to the wrong recipient or the wrong information may be sent if the info being referenced is incorrect.

<u>Mitigation:</u> With no logical connection between the VA email system and EARS, the mitigations used will be the VA encryption techniques and that users will cross reference the correct Affiliate email when the recipient is put into the email.

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?

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.

This Privacy Impact Assessment (PIA) 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." Notice is also provided in the Federal Register with the publication of the SORN 76VA05: Altered System of Records, General Personnel Records (Title 38)–VA.

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

Notice was provided as stated above and is posted in the Appendix. .

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 was provided as stated above and is posted in the Appendix. .

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

Individuals would not have an opportunity to decline to have the information collected. By statute, the information needs to be collected so the academic affiliate can be accurately reimbursed for the HPTs educational activity while on VA rotation.

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.

No consent is required.
Employees and VA contractors are required to provide the requested information to maintain employment or their contract with *VHA*

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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:

<u>Privacy Risk:</u> There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.

<u>Mitigation:</u> This risk is mitigated by the availability of the
The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

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.

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.***

EAR contains information on Clinical trainees that is provided by Academic Affiliates. EAR produces reports that are shared with academic affiliates for the purpose of accurate billing and reimbursement. The affiliates do not have access to EA

In general, Employee information is covered under SORN 76VA05 SYSTEM NAME: Altered System of Records, General Personnel Records (Title 38)–VA which describes the process for accessing records.

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).

It is not exempt

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 system is a Privacy Act System

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.

HPTs would contact their local VA facility Health Professions Education Office, the academic affiliate or the VA HPT program site director to correct information.

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.

HPTs are informed verbally about how to correct information.

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.

HPTs would contact their local VA facility Health Professions Education Office, the academic affiliate or the VA HPT program site director to correct information.

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 members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: Inaccurate information is corrected through the academic affiliate and not VA. We do not generate any information on the HPT. HPT information comes from the affiliate. We never discuss the information received on the HPT from the affiliate with the HPT. Only the affiliate would know and relay to VA if the information is incorrect. Incorrect HPT information does not in any way affect the HPT. It only affects the affiliate's reimbursement. The HPT information is for reimbursement to the affiliate only. If we do not have a disbursement agreement with the affiliate, the HPT's information would never be in this system. We only use this system to track HPTs who are on a disbursement agreement so we can accurately reimburse the affiliate.

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.

Business owner approves access, request for user access goes to DTC and they provision the user within the system. Once approved a verification link will be sent to the user's VA email. The link will allow user to establish credentials for access.

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?

No access will be provided to other agencies.

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.

Disbursement coordinators – edit access
Designated Education Officers – edit access
VA Facility Program Site Directors – Read-only access or possibly edit access in some cases
Office of Academic Affiliations Staff – edit access

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?

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.

No vendors will have access to the system.

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.

No training outside of Talent Management System (TMS) annual mandated training.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Not yet approved
2. *The System Security Plan Status Date:* N/A
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 7/18/2023
5. *The Authorization Termination Date:* 7/17/2026
6. *The Risk Review Completion Date:* 7/17/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate with Privacy

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.***

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)*

Salesforce Government Cloud Plus (SFGCP).

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.*

Service Provider: "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B, Order Number: 36C10B9F0460. CLIN SWF-5700.

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 ancillary data will not be collected.

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.

Yes it is described in the Cloud Service Provider Agreement with Salesforce.

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).

The system does not use RPA

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 they provided in this Privacy Impact Assessment is true and accurate.

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2023.12.05 08:39:51 -05'00'

Privacy Officer, Nancy Katz-Johnson

JAMES BORING

Digitally signed by JAMES BORING
Date: 2023.12.04 14:01:53 -05'00'

Information System Security Officer, James Boring

MICHAEL DOMANSKI

Digitally signed by MICHAEL DOMANSKI
Date: 2023.12.04 13:54:08 -05'00'

Information System Owner, Mike Domanski

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).

OPRM website for SORN: https://www.oprm.va.gov/privacy/systems_of_records.aspx

76VA05 SYSTEM NAME: Altered System of Records, General Personnel Records (Title 38)–VA.
00-18287.pdf (govinfo.gov)

Record Schedule 10-1: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf
NARA website link
VA Directive 6500: VA Publication
VA Handbook 6500.1 Electronic Media Sanitization

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