Privacy Impact Assessment for the VA IT System called:

OEHRM Program Data Repository

VACO

Electronic Health Record Modernization Integration Office (EHRM-IO)

Date PIA submitted for review:

09/15/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.Drake@va.gov	202-632-8431
Information System Security Officer (ISSO)	Momolu Sonie	momolu.sonie@va.gov	608-315-0141
Information System Owner	Cedric Norwood	cedric.norwood@va.gov	(202) 957-2132

Abstract

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

The Office of Electronic Healthcare Record Modernization Program Data Repository (OPD) is an Information System that consists of online training information associated with the courses offered by VA Talent Management System. The system environment consists of components such as workstations, laptops, databases and servers that are owned, managed, and maintained by the facilities. The system provides operational connectivity services necessary to enable users' access to information technology resources throughout the enterprise including those within the facility, between facilities, resources hosted at data centers, and connectivity to other systems. The purpose of the system is to provide a location where current and historical data from TMS can be stored and filtered into views; the developers on the EHRM-IO (Electronic Health Record Modernization Integration Office) PMO (Project Management Office) Knowledge Management team will then access these views in order to create Power BI reports for the Internal VA and Cerner community of users.

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.

OEHRM Program Data Repository, Electronic Health Modernization Integration Office (EHRM-IO)

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

The OEHRM Program Data Repository is a decision support analytical system that offers a single source of truth for EHRM-IO program performance of the Talent Management System, along with other data sources. The purpose of this repository is to create a single source of truth for program data related to training, schedules, etc. that can be accessed by the EHRM-IO Knowledge Management team when building web applications and dashboards. The Dashboards, developed in Power BI, leverage a broad set of data sources (from SharePoint, Excel, and others) to generate a single data model. The insights generated from this model range from program management related performance indicators to technical or functional indicators.

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

Electronic Health Record Modernization-Integration Office (EHRM-IO)

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 OEHRM Program Data Repository is a decision support system. It provides support to VA EHRM-IO management and supports approximately 200+ unique visitors; monthly. These users are primarily located VA-wide but also included Cerner Users.

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

There are a number of data sources that will used as part of the OEHRM Repository. The Talent Management System is supported by SAP Success Factor residing in Amazon Web Service cloud infrastructure which uses an SFTP server as a data repository for the user information, online training courses, curriculum and training actions processed. The sensitivity of the data is moderate due the personal information that is covered under the Privacy Act. If the information is altered in any way, there is very limited damage realized by the individual or organization thus maintaining the overall integrity of the data itself. This data is not critical to the overall mission of the VA.

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

OEHRM Program Data Repository does conduct information sharing.

Talent Management System: The Talent management is a decision support system that provides employees, their supervisors, and human resources and training departments more efficient means to manage every aspect of the human resource management functions by leveraging the commercial-off-the-shelf (COTS) SAP SuccessFactors Human Capital Management (HCM) Suite.

VA Cerner: The VA Cerner is a to help a health organization run smoother, Cerner offers a real-time health system that delivers near-instant data. Not only can this help providers make better care decisions for patients, but it can also improve operational efficiency and care monitoring.

Electronic Health Record Modernization – Integration Office: The OEHRM Program Data Repository System 1.0 is a decision support analytical system that offers a single source of truth for EHRM program performance, providing actionable insight and foresight for leadership and a shared understanding across the program. The Dashboards, developed in Power BI, leverage a broad set of data sources (from Sharepoint, Excel, and others) to generate a single data model. The insights generated from this model range from program management

related performance indicators to technical or functional indicators.

Office of Information and Technology (OIT), electronic permission access system (EPAS) office: The OIT and EPAS systems are IT support systems for maintenance and access.

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.

Only PII data is collected and used by the facilities will be referenced in this document since the repository does not maintain, disseminate, or store information accessed by each facility. The facilities within the repository collect, use, and/or disseminate PII that is maintained and stored within TMS 2.0. There are individual PIAs that contain detailed information on the maintenance, dissemination and sharing practices, and storage of the PII for each Enterprise system accessed by the facilities.

3. Legal Authority and SORN

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

OPM/GOVT-1 https://www.govinfo.gov/content/pkg/FR-2012-12-11/pdf/2012-29777.pdf Authorities in this SORN are: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

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 system is not in the process of being modified

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)

Talent Management System (TMS) Identification Number
Business Email
VA Employee ID: VA employee ID used in HR Smart
Person ID: unique identifier used in Talent Management System
SEC ID: used for Profile Matching

PII Mapping of Components (Servers/Database)

OPD consists of 2 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 OPD 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
vac21dbsopd200	**No**	**Yes**	Personal Phone Number Personal Email Gender Name Talent Management System (TMS) Identification Number Business Phone Number VA Employee ID Person ID SEC ID Business Email Business Address (City, State, Zipcode)	Electronic Permission Access System (ePAS).	Transparent Data Encryption is used to encrypt our Azure SQL Server database in real time using database encryption key which is stored in the database boot record for availability during recovery. At-rest encryption in Data Lake is transparent encryption of data at rest, which is setup during the creation of the storage account. The encryption keys are managed by default The keys are the Master Encryption Key, Data Encryption Key and Block Encryption Key.

					Our windows servers use Transport Layer Security protocol and Perfect Forward Secrecy to protect data Our Linux servers use Secure Shell to connect to Linux VM's. SSH is an encrypted connection protocol.
vac21dbsopd800	**No**	**Yes**	Personal Phone Number Personal Email Gender Name Talent Management System (TMS) Identification Number Business Phone Number VA Employee ID Person ID SEC ID Business Email Business Address (City, State, Zipcode)	Electronic Permission Access System (ePAS).	Transparent Data Encryption is used to encrypt our Azure SQL Server database in real time using database encryption key which is stored in the database boot record for availability during recovery. At-rest encryption in Data Lake is transparent encryption of data at rest, which is setup during the creation of the storage account. The encryption keys are managed by default. The keys are the Master

					Encryption Key, Data Encryption Key and Block Encryption Key. Our windows servers use Transport Layer Security protocol and Perfect Forward Secrecy to protect data. Our Linux servers use Secure Shell to connect to Linux VM's. SSH is an encrypted connection protocol. For in transit, our Windows servers use Transport Layer Security protocol and Perfect Forward Secrecy to protect data. Our Linux servers use Secure Shell to connect to Linux VM's. SSH is an encrypted connection protocol.

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?

OPD collects data from TMS 2.0 Secure File Transfer Protocol server and additional data points are created in OPD.

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 information that resides within the facilities in the repository is collected, maintained, and/or disseminated comes from a variety of sources. For example: items such as name email address and TMS ID are processed by TMS 2.0 applications and shared on the SFTP server.

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

Created values will be maintained in the repository, and therefore it is listed as a source of information.

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?

User Account data from which contains demographic information used to manage user training and development needs is collected through the following means: 1. TMS 2.0 data generated by SQL Success Factor is stored on an SFTP server within an AWS cloud environment. 2. An SFTP connection is established between AWS cloud SFTP server and Azure cloud integration runtime compute infrastructure. 3. The SFTP connection is leveraged to extract data via Azure cloud pipeline to load into Azure cloud SQL Server database.

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.

OEHRM Program Data Repository does not use forms to collect data.

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 that is collected and used directly from enterprise systems have additional details regarding checks for accuracy in their own enterprise level PIAs. Employee, contractor, student, and volunteer information is obtained by automated tools as well as obtained directly by the individuals. The Federal Bureau of Investigation and Office of Personnel Management are contacted to obtain background reviews. Provider credentialing information is obtained from a variety of education resources. Routine daily automated processes are used as a quality control measure to maintain accurate and unique profiles in the OPD system so that VA may reliably deliver various training compliance reports. Discrepancies are resolved through the data validation actions of OPD Administrators. OPD data accuracy is validated by: Executing regular backend scripts and quality control audits that identify issues and, in some cases, resolve them automatically. Distributing the results of the regular backend scripts to each of the team members daily to validate the data against the source record counts. Archiving the source data loaded into a centralized data repository with a data timestamp added to each record for future audits, balance and control of the data migrations. The following data quality goals are the current focus areas for OPD audits: Identify and maintain accurate user email addresses in the OPD system. Identify unique user email addresses within OPD user profiles. Identify unique TMS IDs within OPD user profiles to eliminate duplicate profiles. Identify accurate Program and Role codes for OPD User Profiles. Identify acceptable lifecycle times for programs initiated and completed. Identify and maintain accurate Supervisor/Manager information within OPD user profiles. A series of data quality audits can provide measurable inputs to benchmark targeted process and data improvement areas. The data quality audit measurements will serve to prioritize issues and incrementally bridge the deficiency gaps by embedding quality assurance into processes to achieve an enhanced future state. The data migrated from the TMS SFTP server to OPD databases are compared to the corresponding sources systems for data validation of each source data element. To further ensure the integrity of the data; transformation rules are applied during the data migration into the database server which includes the data characteristics, data limits, default values, last update timestamps and null value management key data value definitions. These data quality measures are reserved in archive files which coincides with last update timestamps and can also serve as recover points in time during data recover and audit exercises.

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.

We do not use a commercial aggregator of information to assess accuracy

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

The legal authorities are 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

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.

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

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

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.

Follow the format below when entering your risk assessment:

Privacy Risk: There is a risk associated with PII data being included in our daily data migration process, either in additional columns or because data was incorrectly entered into a column currently included in the pipeline.

Mitigation: In the event PII data is unintentionally replacing non PII data elements, the data migration process will fail due to inability to meet data quality standards during the reporting process. As a result, the data will never be shared and replaced with the updated data elements.

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/TMS ID/VA Employee ID/Person ID/SEC ID: Used to identify the user registered for a course and in other forms of communication.
Personal/Business Phone Number(s): Used for communication, confirmation of course registration.
Personal/Business Email Address: used for communication.
Business Address: used for communication.
Education Information: Used for demographic background information for veterans and as a determining factor for VA employment in areas of expertise. Basic educational background, e.g. High School Diploma, college degree credentials
Gender: Used as patient demographic, identity and indicator for type of medical care/provider and medical tests required for individual. used for communication.

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.

Although the system itself does not inherently provide such functionality, the supporting OPD relational database could be accessed to perform aggregating analysis using Microsoft Power BI reporting tool. These capabilities are only available to provisioned OPD assigned to the SAVI data and dashboard team

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.

The system aggregates data into a statistical report that will be used in decision making. This aggregation will create a new record that will not be placed individual records but maintained by the system. One purpose of these reports is to identify individuals who have not completed required trainings; therefore, leadership may contact individuals to inform them they need to complete their trainings based on information in these reports.

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?

Transparent Data Encryption is used to encrypt our Azure SQL Server database in real time using database encryption key which is stored in the database boot record for availability during recovery. At-rest encryption in Data Lake is transparent encryption of data at rest, which is setup during the creation of the storage account. The encryption keys are managed by default. The keys are the Master Encryption Key, Data Encryption Key and Block Encryption Key. Our windows servers use Transport Layer Security protocol and Perfect Forward Secrecy to protect data. Our Linux servers use Secure Shell to connect to Linux VM's. SSH is an encrypted connection protocol. For in transit, our Windows servers use Transport Layer Security protocol and Perfect Forward Secrecy to protect data. Our Linux servers use Secure Shell to connect to Linux VM's. SSH is an encrypted connection protocol.

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

Social security numbers are not available within the OPD database.

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

Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.

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?

OPD management restricts the granting of the role that allows OPD administrators to create and assign responsibilities to lower-level OPD administrators. This returns oversight control to the System Ownership level of who can gain access and manage OPD data. OPD Administrators are required to complete role-based training for various levels of administration, all users are required to complete an OPD access form as part of their security awareness and privacy training. Standardized OPD Administrator privileging rules have been established and supported via ePAS, as well as auditing logs and procedures put in place to ensure consistent implementation.

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

Yes

2.4c Does access require manager approval?

Yes

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

We monitor who has access to data at the account level.

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

Information System Owner

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*

Personal Phone Number
Personal Email
Gender
Name
Talent Management System (TMS) Identification Number
Business Phone Number
VA Employee ID
Person ID
SEC ID
Business Email
Business Address (City, State, Zipcode)

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.*

We are following GRS 2.6 Employee Training Records 030 (Individual Training Records), which specifies that documents are temporary and should be destroy[ed] when superseded, 3 years old, or 1 year after separation, whichever comes first, but longer retention is authorized if required for business use. In this case, we are retaining records till the end date of the program for data that is older than 3 years old for use in reports on historical trends.

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.

Schedule: General Record Schedule; Series: 2.6: Disposition Authority: DAA-GRS-2016- 0014-0003 Link: https://www.archives.gov/records-mgmt/grs.html

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

the Department of Veterans' Affairs Directive 6500 VA Cybersecurity Program (January 23, 2019). 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 per VA Directive 6500. Digital media is shredded or sent out for destruction per VA Directive 6500.

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.

Research: the data is used in analytical research.
Testing: the data is not used in testing.
Training: the data is not used in training.

Yes, the Talent Management System Identification Number is encrypted and the use of PII in analytical reports is limited to what is needed to fulfill the business purpose (only using name and TMS number when report does not call for information on gender etc.). Access to reports containing PII is limited to end users with a need to know. Wherever possible, data is aggregated to remove PII.

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:

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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 the information maintained by *OPD* could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released, breached, or exploited for reasons other than what is described in the privacy documentation associated with the information.

Mitigation: To mitigate the risk posed by information retention, *OPD* adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4. The *OPD* ensures that all personnel involved with the collection, use and retention of data are trained in the correct process for collecting, using and retaining this data. A Records Management Officer (RMO), Privacy Officer (PO) and an Information System Security Officer (ISSO) are assigned to the system to ensure their respective programs are understood and followed by all to protect sensitive information form the time it is captured by the VA until it is finally disposed of. Each of these in-depth programs have controls that overlap and are assessed annually to ensure requirements are being met and assist staff with questions concerning the proper handling of information.

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***
Talent Management System	To store in system data lake	Personal Phone Number Personal Email Gender Name Talent Management System (TMS) Identification Number Business Phone Number VA Employee ID Person ID SEC ID Business Email Business Address (City, State, Zipcode)	Azure Data Factory (managed service) is used as an ETL tool to establish a connection to SFTP server to extract the data and load into an Azure SQL Server database.
VA Cerner	To provide overview of super user and end user training captured in the VA TMS system.	TMS ID, Name	Power BI (managed service) is used as a digital reporting tool to visual data extracted from an Azure SQL Server database.
Electronic Health Record Modernization – Integration Office	To provide overview of super user and end user training captured in the VA TMS system.	Personal Phone Number Personal Email Gender Name Talent Management System (TMS) Identification Number Business Phone Number VA Employee ID Person ID SEC ID Business Email Business Address (City, State, Zipcode)	Developers through access to Azure SQl Server; End Users through Power BI report (managed service) is used as a digital reporting tool to visual data extracted from an Azure SQL Server database.
Office of Information and Technology (OIT), electronic	For provisioning user access roles to OPD	Personal Phone Number Personal Email Gender Name	Electronic Permission Access System (ePAS).

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*
permission access system (EPAS) office		Talent Management System (TMS) Identification Number Business Phone Number VA Employee ID Person ID SEC ID Business Email Business Address (City, State, Zipcode)	

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: The internal sharing of data is necessary for individuals to receive benefits at the OPD. However, there is a risk that the data could be shared with an inappropriate VA organization or institution which could result in a breach of privacy and disclosure of PII/PHI to unintended parties or recipients.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.

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***
SAP (Success Factor)	As part of transmission of TMS data	Personal Phone Number Personal Email Gender Name Talent Management System (TMS) Identification Number	National ISA/ MOU	Secure FTP

		Business Phone Number VA Employee ID Person ID SEC ID Business Email Business Address (City, State, Zip Code)		

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: There is a risk of inappropriate access by external parties.

Mitigation: Safeguards implemented to ensure data is not shared inappropriately with organizations are employee security and privacy training and awareness and required reporting of suspicious activity. Users are required to have a zero account and be part of the specific user group to have access to said data.

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 system does not provide notice, notice is given at the point of collection (Talent Management System).

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

Notice provided by system of record
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.

This system does not provide notice, notice is given at the point of collection (Talent Management System).

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.

The OPD only requests information necessary to administer courses to EHRM-IO end users. While an individual may choose not to provide information, this may prevent them from obtaining the necessary training that will prevent them from being assigned the roles required to gain access to the system.

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.

The OPD only requests information necessary to administer courses to EHRM-IO end users. While an individual may choose not to provide information, this may prevent them from obtaining the necessary training that will prevent them from being assigned the roles required to gain access to the system.

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 may not receive notice that their information is being collected, maintained, or disclosed by OPD prior to providing the information to VA.

Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP). Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SOR) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

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.***

An individual wanting notification or access, including contesting the record, should mail or deliver a request to the office identified in the SOR. If an individual does not know the "office concerned," the request may be addressed to the PO of any VA field station VHA facility where the person is receiving care or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420. The receiving office must promptly forward the mail request received to the office of jurisdiction clearly identifying it as "Privacy Act Request" and notify the requester of the referral. When requesting access to one's own records, patients are asked to complete VA Form 10-

5345a: Individuals' Request for a Copy of their Own Health Information, which can be obtained from the medical center or online at https://www.va.gov/find-forms/about-form-10-5345a/.

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).

The system is not exempt from 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 system is not exempt from the Privacy Act

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.

Users must notify their supervisor or respective OPD Administrator to correct erroneous information. Individuals may also directly update in the OPD certain data elements of their user profile including, contact information, employee information and training.

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.

Users are provided this information through direct contact with their supervisor and/or OPD Administrator via email, phone and/or face-to face communication.

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.

Users may always contact their supervisor, OPD Administrator for assistance in correcting whatever issue they may encounter.

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 EHRM-IO end user will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: EHRM-IO end user should contact their immediate supervisor or OPD administrator to gain access to correct or contest their information.

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.

Access is requested utilizing Electronic Permission Access System (ePAS). Users submit access requests based on need to know and job duties. EHRM-IO Supervisor and OPD administrator approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes. Once access is granted, individuals can log into the system(s) through dual authentication, i.e., a PIV card with a complex password combination. Once inside the system, individuals are authorized to access information on a need-to-know basis.

Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel. Access to computer rooms at VA *OPD* is generally limited by appropriate locking devices and restricted to authorized VA IT employees. Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes. Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection at the health care area, or an OIG office location remote from the health care area, is controlled in the same manner.

Access to the *OPD* working and storage areas is restricted to VA employees who must complete both the HIPAA and Information Security training. Specified access is granted based on the employee's functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information System Security Officer (ISSO), local Area Manager, System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information.

End user accounts can also be activated/ deactivated by a OPD Administrator with the appropriate permissions.

Profiles for VA Staff that are being On-Boarded or Off-Boarded by the VA Access Identify Management (IAM) Provisioning team are automatically added (or separated) from the OPD.

The prerequisite for all OPD access is to have a VA Active Directory account associated with a PIV card.

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?

None

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.

User access to OPD falls in three general categories: 1) Developer/Administrator (e.g. - VA employees, contractors, interns, volunteers, etc.) and their supervisors, 2) OPD Administrator users (e.g. System Owners, Project Managers, etc.), and (3) System Administrators (e.g. database administrators, Data Architects, etc.). End users (employees, contractors) are granted access to OPD in one of two ways: An end user must complete a database access form which much be approved by the Project Manager. An EHRM-IO developer/administrator submit a request for a non-email zero account via ePAS to gain system administrative access. In addition to the account submission, the user must also submit a request to be added to the role of each resource within the OPD environment access is needed.

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.

Contractors will have access to the System after completing the VA Privacy and Information Security Awareness training and Rules of Behavior annually. Contractors are only allowed access for the duration of the contract this is reviewed by the privacy officer and the designated Contracting Officer Representative (COR). Per the National Contractor Access Program (NCAP) guidelines, contractors can have access to the System only after completing mandatory information security and privacy training, Privacy and HIPAA Focused Training. Certification that this training has been completed by all contractors must be provided to the employee who is responsible for the contract in question.

Yes – Contractors will have access to OPD after completing mandatory and assigned trainings associated with obtaining an Active Directory account. Contractors accessing OPD are required to undergo a background investigation and public trust clearance, but often contract terms require access to OPD before receiving a public trust clearance. Each respective VA Program Manager and Contracting Officer Representative is responsible for working with their OPD Administrator to monitor contractors' access to OPD.

Additionally, provisioned OPD contractors provide system administration support which includes conducting quality assurance, IT security analysis, database management and incident reporting support. All OPD contractors providing system administration support are required to undergo a background investigation and receive a public trust clearance prior to being granted system administration access. OPD Program Managers and Contracting Officer Representatives review OPD system administration and support contracts, annually.

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 OPD personnel, volunteers, and contractors are required to complete initial and annual Privacy and Security Awareness and Rule Behavior (RoB) training, during New Employee Orientation (NEO) or via TMS. In addition, all employees who interact with patient sensitive medical information must complete the Privacy and HIPAA focused mandated privacy training. Finally, all new employees receive face-to-face training by the System Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officers also perform subject specific trainings on an as needed basis. Each site identifies personnel with significant information system security roles and responsibilities. (i.e., management, system

managers, system administrators, contracting staff, HR staff), documents those roles and responsibilities, and provides appropriate additional information system security training. Security training records will be monitored and maintained. The Talent Management System offers the following applicable privacy courses: VA 10176: Privacy and Information Security Awareness and Rules of Behavior VA 10203: Privacy and HIPPA Training VA 3812493: Annual Government Ethics. All individuals (employees, contractors, interns, volunteers, etc.) who have access to or use VA IT systems or VA sensitive information must complete the federally mandated privacy and information security awareness training and sign the VA National Rules of Behavior. Additionally, OPD Administrators are required to complete specific role-based trainings that includes specific instruction on how to appropriately handle information (including, sensitive information) maintained in OPD.

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

A & A has not been completed.

8.4a If Yes, provide:

1. *The Security Plan Status: A&A Not Completed*
2. *The System Security Plan Status Date: : A&A Not Completed*
3. *The Authorization Status: : A&A Not Completed*
4. *The Authorization Date: : A&A Not Completed*
5. *The Authorization Termination Date: : A&A Not Completed*
6. *The Risk Review Completion Date: : A&A Not Completed*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH): : A&A Not Completed*

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.***

No – The Initial Operating Capability date was granted on 06/19/2006. The current FIPS 199 Classification of the Electronic Healthcare Record Modernization System is Low.

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)*

The system utilizes VA Enterprise Cloud.

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.*

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.

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.

9.4 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).

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**
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.

JULIE DRAKE Digitally signed by JULIE DRAKE
Date: 2023.09.26 07:02:15 -04'00'

Privacy Officer, Julie Drake

Momolu B. Sonie 736101 Digitally signed by Momolu B. Sonie 736101
Date: 2023.09.25 13:33:19 -05'00'

Information System Security Officer, Momolu Sonie

CEDRIC NORWOOD Digitally signed by CEDRIC NORWOOD
Date: 2023.09.25 13:57:43 -04'00'

Information System Owner, Cedric Norwood

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).

HELPFUL LINKS:

National Archives (Federal Records Management):

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

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