Privacy Impact Assessment for the VA IT System called:

Clinical Information Support System & Occupational Health Record-Keeping System

(CISS-OHRS)

Veteran Health Administration (VHA)

Health Services Portfolio, Enterprise Portfolio Management Division (EPMD)

Date PIA submitted for review:

08/25/2023

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)	Ahmed Tamer	Tamer.Ahmed@va.gov	202-578-7559
Information System Owner	Christopher Brown	christopher.brown1@va.gov	202-270-1432

Abstract

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

The Clinical Information Support System & Occupational Health Record-Keeping System (CISS-OHRS) is a web-based portal application. CISS is the login portal that is used to access OHRS. The focus of OHRS is to collect clinical data for immunizations, medical clearance for respirator use, fit testing and training, adverse reactions to medications and pandemic influenza illness.

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.

Clinical Information Support System & Occupational Health Record-Keeping System (CISS-OHRS) Healthcare Environment and Logistics Management (HELM) Product Line.

B. *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
The Clinical Information Support System & Occupational Health Record-Keeping System (CISS-OHRS) is owned by Department of Veterans Affairs (VA), Veterans Health Administration (VHA), Enterprise Operations (EO), Austin Information Technology Center (AITC). **This system has been replaced by Occupational Health Record-Keeping System 2.0 (SF - OHRS2.0) - #2675 and in the process of being decommissioned.**

C. *Indicate the ownership or control of the IT system or project.*
CISS-OHRS is a web-based portal application. CISS is the login portal that is used to access OHRS. The focus of OHRS is to collect clinical data for immunizations, medical surveillance, and adverse drug reactions. OHRS captures and stores information on approximately 350, 000 VA employee patient encounters, (includes everyone working in hospitals and clinics) such as encounter type, purpose, status, provider, and other pertinent clinical data obtained during a patient visit. Users with appropriate security privileges can add and sign or co-sign Occupational Health (OH) encounters and, if needed, perform scheduled and unscheduled reporting on items such as vaccination rates, vaccination status, immunity status and medical clearance to wear respirators. CISS-OHRS does not share patient-specific data but will collect data elements limited to information deemed critical to the Enterprise Occupational Health (EOH) delivery of care processes in the OHRS database. Employee data is obtained from the central Personnel and Accounting Integrated Data System (PAID) while volunteer information is obtained from the Voluntary Service System (VSS). Other Non-Paid and non-VSS data is collected by direct data entry into OHRS at the time of the patient encounter. **This system has been replaced by Occupational Health Record-Keeping System 2.0 (SF - OHRS2.0) - #2675 and in the process of being decommissioned.**

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 OHRS application is also an integral component supporting VA's role in monitoring and tracking the progress of the Occupational Health vaccination program for the non-VA Federal workforce against pandemic influenza including documentation of adverse medication events. The system is accessed by VHA Employee Occupational Health staff who work in VHA health care facilities including medical centers, health care systems and associated outpatient clinics. As part of the American Recovery and Reinvestment Act, all public and private healthcare providers and other eligible professionals were required to adopt and demonstrate "meaningful use" of electronic medical records by January 1, 2014 to maintain their existing Medicaid and Medicare reimbursement levels. 5 CFR 293.502 and 503 define the creation and maintenance of employee medical files. OPM GOVT10 and 08VA05 serve as the system of records documents for employee medical files. The completion of this PIA will not result in circumstances that requires changes to business processes and no funding for any modification. **This system has been replaced by Occupational Health Record-Keeping System 2.0 (SF - OHRS2.0) - #2675 and in the process of being decommissioned.**

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

Occupational Health Record Keeping System (OHR) (Clinical Information Support System & Occupational Health Record Keeping System (CISS-OHRS)) was a web-based portal application replaced by OHR 2.0. Only the database remains which will be decommissioned once VA Records Management rules on the disposition of the remaining patient records. CISS was the portal, through which users gain access to OHRS. The focus of CISS-OHRS was to collect clinical data for immunizations, wellness, medical surveillance, and appropriate treatment of work-based injury or illness. OHRS use to capture and stores information on VA employee patient encounters, such as encounter type, purpose, status, provider, and other pertinent clinical data obtained during the patient visit. Users with appropriate security privileges were allowed to add and sign or co-sign Occupational Health (OH) encounters and, if needed, performs scheduled and unscheduled reporting on items such as vaccination rates, vaccination, and immunity statuses. The OHRS application did not share patient-specific data but would collect data elements limited to information deemed critical to the Occupational Health delivery of care processes in the OHRS database. Employee data is obtained from the central Personnel and Accounting Integrated Data System (PAID) while volunteer information is obtained from the Voluntary Service System (VSS). Other Non-Paid and non-VSS data was collected by direct data entry into OHRS at the time of the patient encounter. The OHRS application was also an integral component supporting VA's role in monitoring and tracking the progress of the Occupational Health vaccination program for the non-VA Federal workforce including documentation of adverse medication events. **This system has been replaced by Occupational Health Record-Keeping System 2.0 (SF - OHRS2.0) - #2675 and in the process of being decommissioned.**

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

Information is not shared and remains in read only status in database.

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.

Not operated at more than one site.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system. PTA 3.5.1

CISS-OHRS operates under System of Record Notice (SORN) 08VA05 (title 38 and hybrid), OPM GOVT10 (title 5), and the Occupational Safety and Health Act of 1970, Public Law 91-596 84 STAT.1590, Title 38, United States Code, Chapter 73, Section 7301.

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?

No. Modifications are not being made to the system and no cloud technology.

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)

The following information is also collected: Occupational Series, Occupational Health, Job title, Service line, Duty station, Supervisors, and Immunizations.

PII Mapping of Components (Servers/Database)

Clinical Information Support System & Occupational Health Record-keeping System consists of one key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Clinical Information Support System & Occupational Health Record-Keeping System and the functions that collect it are mapped 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
vaaussqlohr200	Yes	Yes	Social Security Number, Name, e-mail, address, gender DOB, Job Position, Employee ID	Information is used to track individuals (employees) who are showing signs of contracting the COVID-19 virus or influenza or who have been confirmed as having contracted the virus.	Data is encrypted and will not be transmitted to non-VA storage.

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?

The primary source of personally identifiable information (PII) came from the VA Personnel and Accounting Integrated Data (PAID) system which performs daily exports to the OHRS application. PII is entered into PAID through Human Resources (HR) with consent of the individual – this is not a function of the OHRS application. The data imported from PAID is general HR data such as name, address, SSN, and email.

The second primary source of personally identifiable information (PII) came from the Voluntary Service System (VSS) which performs exports twice a month to the OHRS application. PII is entered into VSS through Voluntary Service with consent of the individual – this is not a function of the OHRS application. The data imported from VSS is general data such as name, address, gender, date of birth. SSN are not collected.

In addition, OHRS had the capability for an authorized system user to manually enter data from the individual directly. Authorized OHRS system users enter information about an individual's

Occupational Health into the system for record. Information typically entered by an authorized user includes medical information, such as immunizations given by VA and treatment for injuries sustained on the job.

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.

N/A

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

N/A

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?

PII\SPI was mainly received via electronic transmission from the PAID or VSS applications. Alternatively, if an individual's information is not available in OHRS at the time of the requested treatment, an OHRS authorized user may collect PII\SPI directly from the individual and enter it manually into the OHRS application. Once a record exists for an individual from one of the three methods above, then an OHRS Version Date: October 1, 2017Page 5 of 43authorized user manually enters health information into the system based on the services rendered to the individual (such as an immunization given).

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.

N/A

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.

OHRS collected and maintained PII\SPI to verify the identity of VA employees, volunteers and trainees, and to track Occupational Health Records of these individuals such as immunizations. This system provides the VA with a method to track Occupational Health Records necessary to ensure the safety of VA Personnel and those they come in contact with by tracking the immunizations and other treatments employees receive. The system does not collect, use, disseminate, or maintain publicly available or commercial 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.

The OHRS application performed weekly record validations to reconcile OHRS database records with those from PAID. The system does not access a commercial aggregator of information. If there is a question whether an individual is already in the system, the record goes to reconcile and a manual process of verifying that they are the same person or not is completed. The end result is to match, create a new patient, or cancel (used if more information is needed before a decision is made). Administrators or OHRS make this determination.

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

CISS-OHRS operates under System of Record Notice (SORN) 08VA05 (title 38 and hybrid), OPM GOVT10 (title 5), and the Occupational Safety and Health Act of 1970, Public Law 91-596 84 STAT.1590, Title 38, United States Code, Chapter 73, Section 7301.

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:
Sensitive employee information may be released to unauthorized individuals.

Mitigation:

- OHRS resides at AITC and is covered by the local GSS so, it adheres to information security requirements instituted by VA Office of Information and Technology (OIT)

- All employees with access to the PII/PHI are required to complete the VA Privacy Information Security Awareness Training and Rules of Behavior, annually.

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.

OHRS tracked Occupational Health Records for VA Employees, Volunteers and trainees. OHRS collects the following information:
Name: Used to identify individual.
Date of Birth: Used to identify individual.
Mailing Address: Used to contact individual if needed.
Race/Ethnicity: Used to identify race and ethnicity.
Gender: Used to identify gender.
Phone Number: Used to contact individual if needed.
Job Title: The Joint Commission requires some reports to include this information.
Service Line: To determine which healthcare personnel in which services are compliant with mandatory programs.
Duty Station: To determine where they are located so the Occupational Health program can report on exposures, adverse health effects, track adverse events; for example, reporting on compliance with influenza vaccination by healthcare facility.
Immunizations: Record of shots given or received previously.
Social Security Number: Used as a patient identifier to be replaced with EIN as soon as VA implements this process. SSN is not collected for volunteers. Other Federal agency employees may substitute their home address for the SSN. Used to identify the patient.
Email address: Used to contact individual if needed.
Occupation Health: Health record that is tracked for VA Employees, Volunteers and trainees.
Occupation Series: This is an occupational code which is used to sort and report on compliance with various mandatory programs (OSHA, TJC etc.).
Supervisors: Enables notifications to be sent to the Employee's supervisor. Eventually, supervisors may have role-based access.

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.

OHRS collected data elements limited to information deemed critical to the Occupational Health (OH) delivery of care. Occupational Health staff may run canned reports. These reports may be a summary (no patient identifiers) or detailed (individual patients). Staff are trained not to release PI or

PHI unless is it authorized by federal regulations or VA/VHA policy. No analysis is done to the data collected. Information is not currently available to others than those inputting health information and occupational health staff.

Under a White House initiative, the VA is required to vaccinate other Federal employees during pandemic events. The VA Pandemic Influenza Plan identifies the federal laws and regulations that allow VHA EOH programs to treat other federal agency employees. The link to the plan is https://www.publichealth.va.gov/docs/flu/pandemic/VAPandemicFluPlan_2006-03-31.pdf Appendix B lists the laws and regulations.

Demographic information (name, SSN, (or address), DOB, gender, agency) is received from those other Federal agencies and entered in to OHRS so that documentation of vaccination can occur. The OHRS application is an integral component supporting VA's role in monitoring and tracking the progress of the Occupational Health vaccination program for the non-VA Federal workforce including documentation of adverse medication events. This functionality would be used only if a national emergency was declared and the VA was directed to support the immunization of other federal agency workers. (Not currently active).

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.

N/A

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?

OHRS is a role-base application. Users must complete training on OHRS in TMS before granted access. Local administrators who are EOH staff physicians, physician assistants, advanced practice registered nurses, and registered nurses, with appropriate training can grant access as can Regional (VISN), and National Administrators. The role determines what information the individual has access to. OHRS has an audit report which identifies active and inactive users and their various roles. National Regional and Local Administrators can grant access. They are required to complete training in TMS on their responsibilities and ensuring that anyone who is granted access has completed the TMS training, and is granted the appropriate role based access e.g. an occupational health physician an OH physician an occupational health nurse practitioner and mid-level provider etc. Administrators can check role-based access by generating reports on who has what role-based access. Currently the data base is set to read only access. (See Appendix B).

CISS-OHRS operated under System of Record Notice (SORN) 08VA05 Title, 38 and the Occupational Safety and Health Act of 1970, Public Law 91-596 84 STAT.1590.

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

Data is encrypted.

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

Data is encrypted.

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?

OHRS is a role-base application. Users must complete training on OHRS in TMS before granted access. Local administrators who are EOH staff physicians, physician assistants, advanced practice registered nurses, and registered nurses, with appropriate training can grant access as can Regional (VISN), and National Administrators. The role determines what information the individual has access to. OHRS has an audit report which identifies active and inactive users and their various roles. National Regional and Local Administrators can grant access. They are required to complete training in TMS on their responsibilities and ensuring that anyone who is granted access has completed the TMS training, and is granted the appropriate role based access e.g. an occupational health physician an OH physician an occupational health nurse practitioner and mid-level provider etc. Administrators can check role-based access by generating reports on who has what role-based access. (See Appendix B).CISS-OHRS operates under System of Record Notice (SORN) 08VA05 Title, 38 and the Occupational Safety and Health Act of 1970, Public Law 91-596 84 STAT.1590.

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?

Yes.

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

VA provides Windows and Unix access controls along with the following security controls: Audit and Accountability, Awareness Training, Security Assessment and Authorization, Incident Response, Personnel Security, and Identification and Authentication. • All personnel with access to OHRS are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. • All personnel with access to OHRS are required to complete OHRS training before access is granted. • OHRS adheres to all information security requirements instituted by OIT. • Information is shared in accordance with VA Handbook 6500.

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*

The following information is retained: full name, SSN, DOB, race, ethnicity, gender, mailing address, occupational series, race/ethnicity, supervisors, occupational health, phone number, job title, service line, duty station and immunizations.

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.

The information in the Occupational Health-Record Keeping System (OHRS) is required for the ongoing healthcare to employees, volunteers, and trainees. These electronic health records (EHR) are retained for 75 years after last instance of treatment or death. This follows the guidelines outlined in Department of Veterans Affairs, Veterans Health Administration, Records Control Schedule (RCS) 10-1, Item No. XLII(b) (March 1, 2011). Records are required to be maintained for 30 years beyond employment.

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?

OHRS follows the guidelines established in the Department of Veterans Affairs, Veterans Health Administration, Records Control Schedule (RCS) 10-1 (March 1, 2011). OHRS operates under System of Record Notice (SORN) 08VA05 (title 38 and hybrid), OPM GOVT10 (title 5), and the Occupational Safety and Health Act of 1970, Public Law 91-596 84 STAT.1590, Title 38, United States Code, Chapter 73, Section 7301. https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf.

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

Currently being determined by the VA Records Manager.

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.

If an employee transfers to another federal agency, OHRS is required to send any health records to the gaining agency. When an employee retires their record must be sent to the National Archives. In

both situations all documents must be printed and placed in the Employee Medical File for transfer. All original information remains in OHRS and will be kept for 30 years beyond employment, in accordance with OHSA regulations. Therefore, any disposing of records would follow NARA protocols. In OHRS, patients are identified as separated and no one should go in to those records. If they do, they need to identify why and an audit trail is kept. There are no rules around deleting any health information after the required timeframe, no funding was received to accomplish this task.

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.

Yes. Research is not conducted in EOH where OHRS is utilized. Testing of the system is not done in production and training is not done in production.

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:

<u>Privacy Risk:</u>

There is a risk that the information contained in OHRS will 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 or breached.

Mitigation:
OHRS retains only the information that is necessary to ensure the continuity of care for employees, contractors, and volunteers who seek medical treatment related to their work at the VA. Additionally, the information is kept in accordance with NARA approved record schedules and securely destroyed at the end of the retention period.

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.

Information list below is how data was collected and shared. Data that was collected remains in the current read only database and no longer is shared or additional data collected.

Data Shared with Internal Organizations

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

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk:
If appropriate safeguards are not in place, then Privacy information shared within the Department may result in unauthorized data access.

Mitigation:
Release of PII to unauthorized individuals is prohibited by the Privacy standards mandated to all VA employees, affiliates, trainees, volunteers, and contractors. Both contractor and VA employees are required to take Privacy, Health Insurance Portability and Accountability Act Version Date: February 27, 2020 Page 15 of 28 (HIPAA), and information security training annually. Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training, 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 for the system. The VA Salesforce Business Module Owner defined the software product configuration requirements to customize data access needs for each role category, as well as limiting access within organizational boundaries.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

5.2 <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:

Privacy Risk:
There is a risk that information may be shared with an unauthorized VA program, system, or individual.

Mitigation:
Safeguards implemented to ensure data is not shared with unauthorized individuals are employee security and privacy training and awareness; required reporting of suspicious activity; use of secure passwords; access for need to know basis; encryption; and access authorization, are all measures that are utilized within the facilities.

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.

A laminated copy of the privacy notice is posted in each office. A hard copy is also kept in a folder at the front desk. If an individual request a personal copy of the notice, OHRS will provide one to the individual requesting it. In accordance with Health Insurance Portability and Accountability Act

(HIPAA), VA provides notice to Veterans as a health plan and is required to make notice available upon enrollment into the plan. In addition, VA mails a copy of privacy practices to Veterans every three years. In accordance with HIPAA, VA provides notice to employees as a health care provider and must offer the notice at each episode of care and receive acknowledgement.

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

N/A
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.

N/A

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 do not have the opportunity to decline to provide information to OHRS since the information is gathered from the PAID system and PAID pulls information from several other systems.

For individuals whose information is collected during an appointment they may substitute their SSN with their home address. Identity Management requires five items to ensure correct identity (first name, last name, gender, DOB, and SSN. If no SSN is not available, then substitute with home address).

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.

OHRS only used data to provide VA employees, volunteers, and trainees with medical treatment. It pulls data from PAID and then data is shared with the DSS system (as discussed in section 4 above). Data may be released without consent are covered under systems of records (SOR) OPM GOVT10 (title 5) and 08VA05 (title 38 and hybrid). If the disclosure is not covered under the two SORs then a

release of information form (VA Form 10-5345 or VA Form 10-5345a) must be obtained before information is released.

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 VA employees, trainees, volunteers and contractors will not know the OHRS exists and that it contains information about them.

Mitigation:
The VA mitigates this risk by providing notice of OHRS via A System of Record Notice (SORN), a notice posted in all offices, and a Privacy Impact Assessment (PIA), as discussed in question 6.1. In addition, occupational health staff according to the VHA Notice of Privacy Practices must offer employees the opportunity to read and ask questions every time they are seen in occupational health and sign a form acknowledging they were given the opportunity. This is filed in their medical record and facility Privacy Officers are responsible for conducting audits.

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.

VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 7(b) states the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to, and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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).

N/A

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.

N/A

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.

Under the jurisdiction of VHA, VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 8 states the rights of the Veterans to amend to their records via submitting VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

Notification for correcting the information must be accomplished by informing the individual to whom the record pertains by mail. The individual making the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. The System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee, must notify the relevant persons or organizations that had previously received the record about the amendment. If 38 U.S.C. 7332-protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible,in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

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.

Individuals may inquire about corrections when reviewing their record with an OHRS authorized user at the time of medical treatment. In addition, individuals may contact their HR department or Voluntary service to correct information that gets imported into OHRS from PAID and VSS respectively. Individuals may also contact OIT Product Development (PD) Point of Contact for OHRS.

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:
Because there is no direct way for individuals to review or correct their information in OHRS, there is a risk that the system may use inaccurate data.

Mitigation:
Individuals cannot gain direct access to their information, but can submit a request, as listed in 7.2, for correcting 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.

No one from another agency has been granted access nor would they be granted access to CISS-OHRS. Therefore, the criteria for what PII can be shared is not needed. The CISS-OHRS User Guide says the following: To use the CISS application, you must have:

1. Access to the Veterans Health Administration (VHA) Intranet via Microsoft Internet Explorer version 6.0 or higher, with Service Pack (SP) 2.
2. Standard 128-bit encrypted security (SSL) implemented on your computer - your system administrator can help if you do not know how to install it.

3. The latest version of Flash Player installed on your computer; if you do not have it installed, a message displays, instructing you to contact your Information Resource Management (IRM) point of contact to get the correct version of Flash Player installed
4. An authorized user account that includes a defined user role within the application.
Before an authorized account is granted, a user must complete VA Privacy Awareness Training, VA Information Security Awareness Training, HIPPA training, as well as OHRS training. Once the training has been completed and access has been approved, National, Regional and Local administrators can grant access. Role based Access is then provided. The role is determined by the position for which the individual is assigned to in occupational health e.g. OH provider, OH midlevel provider, RN, PN, NA, tech, clerk or roles in support of occupational health e.g. infection control, wellness nurse, immunization nurse. There is a CRUD matrix (Create, Read, Update, and Delete) Matrix which identifies the actions each of the roles can perform, (feature, encounter, report etc).

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?

N/A

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.

N/A

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. Contractors no longer have access to PII.

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.

New team members must complete VA Privacy Awareness Training, VA Information Security Awareness Training. CISS-OHRS users must complete OHRS training in TMS prior to being granted role-based access to the system.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approve
2. *The System Security Plan Status Date:* 07-18-2023
3. *The Authorization Status:* 07-06-2023
4. *The Authorization Date:* 10-28- 2022
5. *The Authorization Termination Date:* 10-28-2023
6. *The Risk Review Completion Date:* 10-21-2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* MODERATE

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)*

No

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.*

N/A

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.

N/A

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.

N/A

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

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the

automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2023.12.18 14:06:53 -05'00'

Privacy Officer, Nancy Katz-Johnson

TAMER AHMED

Digitally signed by TAMER AHMED
Date: 2023.12.18 14:28:21 -05'00'

Information System Security Officer, Ahmed Tamer

CHRISTOPHER BROWN

Digitally signed by CHRISTOPHER BROWN
Date: 2024.01.22 10:16:22 -06'00'

Information System Owner, Christopher Brown

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).

https://www.va.gov/privacy-policy

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