Privacy Impact Assessment for the VA IT System called:

Advanced Cloud Hosting Environment for ORD (ACHORD)

Veterans Health Administration (VHA)

Office of Research and Development (ORD)

eMASS ID #: 2517

Date PIA submitted for review:

11 September 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Michelle Christiano	michelle.christiano@va.gov	706-399-7980
Information System Security Officer (ISSO)	Erick Davis	erick.davis@va.gov	512-326-6178
System Steward	Bryan Buchta	Bryan.Buchta@va.gov	913-368-8811
Information System Owner	Dr. Jeffrey P. Ferraro	jeffrey.ferraro@va.gov	801-582-1565

Abstract

The abstract provides the simplest explanation for "what does the system do?".

The Office of Research & Development (ORD) Advanced Cloud Hosting Environment for ORD (ACHORD) is an environment consisting of cloud infrastructure, system software (i.e., application servers, database servers), and network resources to ensure that applications and tools can be deployed, monitored, and managed in a standard way. It is a standardized environment that will support various Technical Reference Model (TRM) approved commercial-off-the-shelf (COTS) products, as well as custom developed tools and applications for ORD. This environment will be specifically used to host tools and applications in a standard way, following industry best practices. The general tenets of this environment include: 1. ORD technical staff managing the care and feeding of this environment, as well as the tools and applications deployed in the environment. 2. Standardized DevSecOps Supporting Processes 3. Standardized DevSecOps Software Tools 4. Generalized Stress Testing Environment 5. Monitoring Portal 6. Environment Monitoring Tools This environment is intended to host tools and applications specific to ORD that are currently distributed throughout the VA in different environments with variability across how these tools and applications are operationally managed. The intent is to standardize and leverage best practices for hosting tools and applications developed/deployed by ORD.

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. What is the IT system name and the name of the program office that owns the IT system?

IT System: Advanced Cloud Hosting Environment for ORD (ACHORD)
Program Office: Office of Research and Development

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

For more than 95 years, the Veterans Affairs (VA) Research and Development program has been improving the lives of Veterans and all Americans through health care discovery and innovation. The mission of VA Research is fourfold:

- to improve Veterans' health and well-being via basic, translational, clinical, health services, and rehabilitative research;
- to apply scientific knowledge to develop effective individualized care solutions for Veterans;

- to attract, train, and retain the highest-caliber investigators, and nurture their development as leaders in their fields; and
- to assure a culture of professionalism, collaboration, accountability, and the highest regard for research volunteers' safety and privacy.

VA Research is unique because of its focus on health issues that affect Veterans. It is part of an integrated health care system with a state-of-the-art electronic health record and has come to be viewed as a model for superior bench-to-bedside research.

Today, VA Research has five overarching strategic priorities: increasing Veterans' access to high-quality clinical trials; increasing the real-world impact of VA research; putting VA data to work for Veterans; actively promoting diversity, equity, and inclusion; and building community through VA research.

The Office of Research and Development consists of four research services that together form a cohesive whole to explore all phases of Veterans' health care needs. Each service oversees a number of research centers of excellence.

- Biomedical Laboratory Research & Development Service
- Clinical Science Research & Development Service
- Cooperative Studies Program
- Health Systems Research
- Rehabilitation Research & Development Service

The purpose of ACHORD is to provide a cloud-based standardized and secure development, testing, and hosting environment for ORD applications and tools.

C. Who is the owner or control of the IT system or project?

Veteran Affairs (VA) Office of Research and Development (ORD)

2. Information Collection and Sharing

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

ACHORD's sub-tenants will contain Sensitive Personal Information (SPI) including Personal Identifying Information (PII) and/or Personal Health Information (PHI) on Veterans and VA employees. The total number of Veterans and VA employees can vary and will be dependent on the sub-tenant application or tool being hosted. Hosted information systems will have connectivity and access to the Corporate Data Warehouse (CDW), which contains three billion unique records but not all hosted information systems will utilize the connectivity and access.

E. What is a general description of the information in the IT system and the purpose for collecting this information?

ACHORD sub-tenant applications could contain clinical information on Veterans. In addition, sub-tenant applications may support ORD back-office operations which may contain information about Veterans and VA employees, and VA proposed projects. The information that is collected will be for the sole purpose of these programs and projects.

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

ACHORD is a hosting environment for Office of Research and Development (ORD) tools and sub-applications. The ACHORD hosting environment will share any information due to its nature. However, the sub-applications and tools hosted in the environment as sub-tenants may or may not share information. As new applications are implemented into the hosting environment, the PTA and PIA will be updated to include these technologies as well as any sharing by those systems.

G. Is the system operated at 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?

ACHORD will be hosted in the Veterans Affairs Enterprise Cloud (VAEC) but will be accessed nation-wide by VA employees and contractors through the VA's standard PIV authentication and authorization security controls.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

System of Records Notice (SORN) 34VA12 Research SORN Veteran, Patient, Employee, and Volunteer Research and Development Project Records—VA (34VA12). scription. Link: https://www.govinfo.gov/content/pkg/FR-2021-06-23/pdf/2021-13141.pdf

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

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

4. System Changes

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

No

K. Will 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. It must also match the information provided in question 3.4 of the PTA.

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[1]
- ☒ 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)

Other SPI including PII/PHI data elements: ACHORD is a hosting environment for the Office of Research and Development. At this time, it is not possible to list every data element that will be

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

collected by applications/information systems that will eventually be hosted in this environment as sub-tenants. Known other elements include:

- Finger or voice print
- Photographic image - Photographic images are not limited to images of the face.
- Any other characteristic that could uniquely identify the individual
• Title
• User Id
• Facility Identifier
- Device identifiers and serial numbers
- Web URL

PII Mapping of Components (Servers/Database)

ACHORD itself consists of zero (0) key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect SPI including OHI and PII. The table below is blank as there is no type of SPI collected by ACHORD.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**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**
1) ACHORD Sub-Tenant Applications and Databases 2) VA Electronic Determination Aid	Yes	Yes	*All HIPAA Protected Identifiers* - *Name* - *Address (all geographic subdivisions smaller than state, including street address, city county, and zip code)* - *All elements (except years) of dates related to an individual (including birthdate, admission date,*	For use by the sub-tenant applications based on the functions they are providing to end-users.	All PII/PHI is encrypted and stored on VA encrypted database systems requiring PIV authentication and authorization in accordance with VA security policies.

			discharge date, date of death, and exact age if over 89) - *Personal Phone numbers* - *Personal Fax number* - *Email address* - *Social Security Number* - *Medical record number* - *Health plan beneficiary number* - *Account number* - *Certificate or license number* - *Vehicle identifiers and serial numbers, including license plate numbers* - *Device identifiers and serial numbers* - *Web URL* - *Internet Protocol (IP) Address* - *Finger or voice print* - *Photographic image - Photographic images are not limited to images of the face.* - *Any other characteristic that could uniquely identify the individual* Additional Information		

			- Mother's Maiden Name - Emergency Contact Information (Name, Phone Number, etc. of a different individual) - Medications - Medical Record - Race/Ethnicity - Gender - Integrated Control Number (ICN) - Military History/Service Connection - Next of Kin		

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 sub-tenant applications may support ORD back-office operations which may contain information about Veterans and VA employees, and VA proposed programs and research projects. There are research projects that will obtain data to be included in ACHORD; however, the full sources of information are currently unknown.

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 ACHORD environment may also host applications related to storing information about proposed research projects, policy documents, and VA enterprise-wide programs and projects.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

No. ACHORD as a hosting environment does not create 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?

Yes. Information may be collected from individuals (Veterans and VA Employees) as well as accessed via the CDW or data provided by individual research projects or programs.

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

No.

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.

While ACHORD does not assume responsibility for the safekeeping of CDW data—this remains outside the scope of ACHORD's duties—the integrity of the systems within the ACHORD environment is rigorously maintained. Applications hosted in the ACHORD environment are subjected to stringent industry-standard testing and validation protocols. These processes are meticulously designed to ensure that all systems function correctly and securely, safeguarding the data they process and maintaining the highest levels of operational reliability.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

No, there is no commercial aggregator of information.

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

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

The legal authority for ACHORD is under the

System of Records Notice (SORN) 34VA12 Research SORN Veteran, Patient, Employee, and Volunteer Research and Development Project Records—VA (34VA12). scription. Link: https://www.govinfo.gov/content/pkg/FR-2021-06-23/pdf/2021-13141.pdf

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

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: A HIPAA violation within the VA would have serious implications, including legal penalties and potential lawsuits from Veterans whose privacy has been compromised. The VA could face fines in accordance with HIPAA violation policies. Beyond legal consequences, the violation could disrupt VA operations due to mandatory audits, investigations, and the need for corrective actions, such as revising policies and enhancing security measures. The VA's reputation could also suffer, leading to a loss of trust among Veterans and public scrutiny, which could impact funding and support.

Mitigation: All of the VA security controls at a moderate categorization will be implemented to include the Privacy Overly, which are additional Security Controls added to the eMASS

packaged specifically related to protecting privacy information. These added Security Control help prevent a breach of PII/PHI information.

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 that 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.

PII/PHI Data Element	Internal Use	External Use
Name	Individual identification	Not used
Social Security Number	Individual identification	Not used
Date of Birth	Individual identification	Not used
Mother's Maiden Name	Individual identification	Not used
Personal Mailing Address	Individual identification and communication	Not used
Personal Phone Number	Individual identification and communication	Not used
Personal Fax Number	Individual identification and communication	Not used
Personal Email Address	Individual identification and communication	Not used
Emergency Contact Information	Emergency contact	Not used
Financial Information	Not Used	Not used
Health Insurance Beneficiary Numbers	Individual identification	Not used
Account Number	Individual identification	Not Used
Certificate/License Numbers	Individual identification	Not used
Vehicle License Plate Numbers	Vehicle association to individual or family	Not used
Internet Protocol (IP) Address	Audit records / logs	Not used
Device identifiers and Serial numbers	Audit records / logs	Not used
Web URL	Audit records / logs	Not used
Finger or voice print	Audit records / logs	Not used
Photographic Image	Individual identification	Not used
Medications	Individual identification Individual identification	Not used
Medical Records	Individual identification	Not used
Race/Ethnicity	Individual identification	Not used
Tax Identification Number	Not Used	Not used

Medical Record Number	Individual identification	Not used
Gender	Individual identification	Not used
Integrated Control Number	Individual identification	Not used
Military History / Service Connection	Individual identification	Not used
Next of Kin	Individual identification	Not used

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?

ACHORD is a hosting environment and does not analyze data, it hosts sub-tenant applications and tools. The sub-tenant applications and tools hosted in ACHORD may perform any of the above activities.

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.

No sub-tenant system will update an individual's medical record.

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?

All of the VA security controls at a moderate categorization will be implemented to include the Privacy Overly, which are additional Security Controls added to the eMASS packaged specifically related to protecting privacy information. These added Security Control help prevent a breach of PII/PHI information. ACHORD will be hosted on the VA Enterprise Cloud (VAEC), which is FedRAMP certified and ACHORD will inherit the Security Controls of the VAEC environment.

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

Encryption for data at rest and in process in accordance with VA security policy and guidelines. This will be inherited from the VAEC cloud environment.

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

All of the VA security controls at a moderate categorization will be implemented to include the Privacy Overly, which are additional Security Controls added to the eMASS packaged specifically related to protecting privacy information. These added Security Control help prevent a breach of PII/PHI information. ACHORD will be hosted on the VA Enterprise Cloud (VAEC), which is FedRAMP certified and ACHORD will inherit the Security Controls of the VAEC environment. Access to the PII/PHI in hosted applications is determined by the authorized individual have a public trust clearance, appropriate authorized role, need-to-know, requisite PII training, and potentially additional requirements as determined by the ORD.

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?

The ACHORD environment itself does not collect, store, or process PII for any user. However, some of the sub-tenant applications and tools hosted in the environment do collect, store and/or process PII. Access to the PII in hosted applications is determined by the authorized individual have a public trust clearance, appropriate authorized role, need-to-know, requisite PII training, and potentially additional requirements as determined by the ORD.

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

ACHORD is a hosting environment and does not work with PHI or PII. Sub-tenant applications hosted in this environment will be responsible for maintain adequate documentation in accordance with VA policies and procedures.

2.4c Does access require manager approval?

The ACHORD hosting environment will be managed by ORD senior operational staff that must approve and provision sub-tenant environments for candidate applications and tools.

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

The VA Corporate Data Warehouse (CDW) continuously monitors and tracks access to the data stored within this enterprise database system, ensuring the integrity and security of the information. For personally identifiable information (PII) that is stored within sub-tenant application databases, the responsibility shifts to the application development group. It is their duty to implement robust electronic monitoring and tracking mechanisms for PII within their respective application databases. This ensures that any access or usage of sensitive information is carefully logged and audited, maintaining compliance with security protocols and protecting the privacy of individuals whose data is stored within these systems.

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

The sub-tenant operational support teams are responsible for assuring safeguards for PII or PHI used or stored by their application(s).

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 ACHORD hosting environment does not retain any information. Instead, sub-tenant applications and tools are responsible for retaining any data, ensuring compliance with relevant research guidelines and VA policies.

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 ACHORD hosting environment does not retain any information. Instead, sub-tenant applications and tools are responsible for retaining any data, ensuring compliance with relevant research guidelines and VA policies.

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?

The ACHORD hosting environment does not retain any information. Sub-tenant applications and tools are responsible for setting and enforcing data retention policies in line with applicable research guidelines and VA regulations. Individual VA research projects must comply with Records Control Schedule 10-1.

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

The ACHORD hosting environment does not retain any information. Sub-tenant applications and tools are responsible for setting and enforcing data retention policies in line with applicable research guidelines and VA regulations. Individual VA research projects must comply with Records Control Schedule 10-1.

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.

In the ACHORD hosting environment, the responsibility for the elimination or transfer of Sensitive Personal Information (SPI) lies with the sub-tenant applications and tools, not with ACHORD itself.

When SPI reaches the end of its mandatory retention period, each sub-tenant application must ensure that records are either securely destroyed or transferred in accordance with relevant privacy controls, mandatory retention period as noted in Records Control Schedule 10-1, legal requirements and VA policies.

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.

In the ACHORD hosting environment, sub-tenant applications that host research involving human participants and/or their Personally Identifiable Information (PII) for testing, training, or research purposes are required to adhere strictly to VA Privacy requirements, VA security guidelines and Institutional Review Board (IRB) requirements.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: ACHORD is a hosting environment that does not retain any data itself. The responsibility for managing data, including addressing privacy risks and adhering to security policies, falls to the sub-tenant applications operating within ACHORD. The length of time that data is retained can pose significant privacy risks. This retention period must align with the Privacy Act's requirements to retain only the minimum amount of PII necessary for the specified purposes, as well as the Federal Records Act. Proper management of PII is critical to avoid potential privacy violations including HIPAA, which could result in legal repercussions, financial penalties, and damage to organizational reputation.

Mitigation: To mitigate these privacy risks, sub-tenant applications must implement and adhere to strict data retention policies and procedures including Records Control Schedule 10-1. These policies ensure that PII is retained only for the minimum amount of time required to fulfill its intended

purpose. Additionally, sub-tenant applications must have robust mechanisms for purging PII that is no longer relevant, following the principles of data minimization and data quality and integrity. By adhering to these practices, sub-tenant applications help ensure compliance with privacy controls DM-1 and DM-2, thus protecting PII and reducing associated risks.

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***
Office of Research and Development (ORD)	A sub-tenant application may have a backend database component where it stores information related to the application.	*All HIPAA Protected Identifiers* - *Name* - *Address (all geographic subdivisions smaller than state, including*	Transmission to and from the database to the application server will be done over an encrypted

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*
		street address, city county, and zip code) - *All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)* - *Personal Phone numbers* - *Personal Fax number* - *Email address* - *Social Security Number* - *Medical record number* - *Health plan beneficiary number* - *Account number* - *Certificate or license number* - *Vehicle identifiers and serial numbers, including license plate numbers* - *Device identifiers and serial numbers* - *Web URL* - *Internet Protocol (IP) Address* - *Finger or voice print* - *Photographic image - Photographic images are not limited to images of the face.* - *Any other characteristic that could uniquely identify the individual* Additional Information - Mother's Maiden Name - Emergency Contact Information (Name,	database channel within the VA network. In addition the electronic presentation of information from the application server to the front-end browser will be done using a TLS encrypted channel. Access to all applications will require PIV authentication and authorization.

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*
		Phone Number, etc. of a different individual) - Medications - Medical Record - Race/Ethnicity - Gender - Integrated Control Number (ICN) - Military History/Service Connection - Next of Kin	

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: A HIPAA data breach poses a significant privacy risk as it can expose sensitive personal information (SPI) including protected health information (PHI). Such breaches may lead to identity theft, financial fraud, or other forms of harm, compromising individuals' personal and medical privacy.

Mitigation: This risk is minimal in our case, as we will follow VA security protocols. These protocols include encryption, strict access controls, and routine security audits, all designed to safeguard patient information and ensure full compliance with privacy regulations, thereby reducing the likelihood of a breach.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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 no external sharing of information.

Mitigation: There is no external sharing of information.

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.

There are no notices provided to individuals. Any sub-tenant application will follow VA policies related to notification of use of individual information stored within the VA Health System. Research projects will provide the IRB approved participant facing document such as an information sheet, informed consent form/document, VA Form 10-0493 and for non-Veterans enrolled in the individual research project, a Notice of Privacy Practice (NOPP) must be provided. The Veterans Benefit Administration (VBA) provides a NOPP to all enrolled Veterans every three years.

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

There are no notices provided to individuals as ACHORD does not interact or intervene with individuals as a hosting environment. Any sub-tenant applications including individual research projects will follow VA policies related to notification of use of individual information.

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.

Any sub-tenant applications of the ACHORD hosting environment will follow VA policies related to notification of use of individual information.

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.

ACHORD is a tenant/sub-tenant environment that hosts applications that support ORD research projects or programs as well as back-office processes. The individual applications that will be hosted in the ACHORD environment will follow VA policies around the collection of any data or information.

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.

ACHORD as a hosting environment does not interact with the individual. Each research project will provide the IRB approved participant facing document such as an information sheet, informed consent form/document, and/or the VA Form 10-0493 as each research project is responsible for their data. Patient healthcare data is maintained by the VHA and ACHORD does not interact with individual patients.

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

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

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

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: The potential risks associated with insufficient notice in healthcare data practices include lack of patient awareness about how their data is being used or shared, which could lead to unauthorized access or use of personal health information. This can result in privacy violations, legal liabilities, and diminished trust in healthcare providers.

Mitigation: To mitigate these risks, the VHA has clear consent processes, providing detailed privacy notices, and enhancing transparency in data usage practices. Compliance with regulations such as HIPAA also help ensure that patients are adequately informed and their data is protected.

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.***

In building ACHORD, a tenant/sub-tenant hosting environment for the VA, our program adheres to established procedures that regulate access to information, including those outlined under the Freedom of Information Act (FOIA) and the Privacy Act.

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.

The operational support team associated with each sub-tenant environment will be responsible for ensuring the accuracy of information. Each sub-tenant support team will be recorded by the operational staff of the ACHORD environment.

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.

The ACHORD hosting environment will host sub-tenant applications. All activities related to a sub-tenant will be handled by the sub-tenant operational support team.

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.

N/A

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: The risks related to the Department's access, redress, and correction policies for ACHORD sub-tenant applications are minimal, as these applications are designed with privacy and security controls in accordance with VA operating policies.

Mitigation: Mitigation of the minimal risks related to the Department's access, redress, and correction policies for ACHORD sub-tenant applications includes implementing privacy and security controls in accordance with VA operating policies. These controls limit access to sensitive data and ensure accuracy through data governance practices.

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 to the ACHORD sub-tenant environment and its sub-tenant applications will be controlled through the VA's SSOi and SSOe PIV security methods. ORD is developing a tool that will be released in Dec 2024 called SWIFT - Simplified Workflow to Inform and Find Technology. ACHORD will be added into this decision support tool. The ACHORD operational support team will configure and grant access to approved sub-tenant operational staff through the standard security controls provided by the VAEC.

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

No other agencies will have access to the ACHORD environment.

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.

All access to the ACHORD tenant/sub-tenant environment will be based on authentication and authorizations rights granted by the sub-tenant applications.

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.

Any contractor personnel who are a part of the support team for a sub-tenant environment will come through an approved VA contract vehicle and must be granted PIV card access rights in accordance with their job responsibilities.

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 privacy training is mandated by the VA and is a core component of the employment agreement for all VA personnel. It includes annual compliance and is documented in the TMS system with a certificate of completion for individuals who complete the required training. This training is designed to ensure that employees are fully informed about privacy regulations, data protection policies, and their responsibilities in safeguarding sensitive information. The VA's structured privacy training program covers relevant laws, policies, and best practices, equipping staff with the knowledge needed to handle personal and confidential data appropriately and comply with federal privacy requirements.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* In Progress
2. *The System Security Plan Status Date:* In Progress
3. *The Authorization Status:* In Progress
4. *The Authorization Date:* In Progress

5. *The Authorization Termination Date:* In Progress
6. *The Risk Review Completion Date:* In Progress
7. *The FIPS 199 classification of the system (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.***

June 2025

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)*

ACHORD will utilize the VA Enterprise Cloud (VAEC).

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

ID	Privacy Controls
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.

MICHELLE CHRISTIANO

Digitally signed by MICHELLE CHRISTIANO
Date: 2024.10.17 12:28:46 -04'00'

Privacy Officer, Michelle Christiano

ERICK DAVIS

Digitally signed by ERICK DAVIS
Date: 2024.10.22 10:32:36 -05'00'

Information System Security Officer, Erick Davis

JEFFREY FERRARO (Affiliate)

Digitally signed by JEFFREY FERRARO (Affiliate)
Date: 2024.10.22 15:27:11 -06'00'

Information System Owner, Jeffrey Ferraro

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; screen shot of a website collection privacy notice).

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

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