Privacy Impact Assessment for the VA IT System called:

ARCHES

OFFICE of HEALTHCARE INNOVATION and LEARNING
VHA

Date PIA submitted for review:

08/25/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	LaWanda Wells	Lawanda.Wells@va.gov	202-632-7905
Information System Owner	Angela Gant-Curtis	Angela.gant-curtis@va.gov	540-760-7222
Project Manager	Amanda Purnell	Amanda.Purnell@va.gov	314-224-9885

Abstract

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

Arches is a data platform where users can readily access usable data to improve care for Veterans. The cloud-native platform, complete with a rich set of computational tools, harnesses the power of collaboration and innovation to provide a one-stop data workshop for Veterans Affairs (VA) employees. Users can easily work together to produce solutions that drive the quality of patient treatment and outcomes. The Arches platform will provide on-demand access to understanding care pathways through the use of automatic synthetic (artificial) data generation, dramatically increasing the ability to use data to improve quality and operations for patient care. The Arches platform includes: a self-service user interface; a data lake that can incorporate and meaningfully organize diverse large data sets; synthetic data generation with metrics on validity and privacy of data outputted; clearly defined data and rules/logic to include measures of sensitivity and specificity; unlimited additional users will have access to user interface for quality assurance and clinical improvement purposes; and collaboration with other users of the Arches platform, creating large, privacy preserving healthcare data sets to unlock insights and provide improvements to care.

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *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.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a System of Record Notice (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?*

Arches is a platform adopted by Veterans Health Administration (VHA) Office of Healthcare Innovation and Learning (OHIL) Innovation Ecosystem (IE) in support of program office stakeholders. The Arches Platform allows for testing, development and validation of early-stage projects and collaborations prior to enterprise scale.

The platform is capable of ingesting a variety of complex data from multiple Veterans Affairs (VA) sources into a single longitudinal database; including the capability for data aggregation from multiple VA and non-VA data sources of unstructured and structured data including the Corporate Data Warehouse (CDW), Patient Generated Health Data (PGHD), genomic, event data, and social determinant as well as data organization into a patient specific longitudinal structure enabling Veteran journey and timeline analysis of all available data. The expected number of individuals whose information is stored in the system is approximately 25 million. The platform includes the capability to administratively manage users of the system using SSOI (single sign-on) in compliance with VA rules and regulations.

Once hosted in the VA Enterprise Cloud (VAEC) environment (Cloud Technology Services) all VA facilities will be able to utilize Arches. Arches has successfully completed the processes to obtain an initial and subsequent Authority to Operate (ATO) within the VAEC. Authority to operate: Title 38 of U.S. Code section 201. The change in the business process will be that VA Stakeholders will be able to readily access usable data to improve care for Veterans. The Arches platform will provide on-demand access to understanding care pathways through the use of automatic synthetic (artificial) data generation, dramatically increasing the ability to use data to improve quality and operations for patient care. VA Stakeholders will be able to use the self-service portal to query the underlying datasets, with automatic synthetic data generation outputs, thereby protecting the privacy and information security of the underlying data. The relevant System of Record Notices (SORN) is 172VA10 VHA Corporate Data Warehouse-VA https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf .

Arches includes a variety of applications to include Synthetic Patient Data, OpenShift, Cluster Modeling, VA Foresight. Expiration Terms of Service (AOSEN/ETS-SP) is a minor application that has its own PTA but it falls under the Arches PIA.

Arches is hosted in the VA Enterprise Cloud, does not hold a FedRAMP status, and has completed an initial and subsequent ATO, with next review due 7/26/2023. The Dept. of Veteran Affairs maintains ownership and rights over all data. The VA Enterprise Cloud contract includes language and processes for security and privacy of data. The security characterization for Arches has been scored as a MODERATE impact system.

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, Information Technology (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 Account Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers

☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Current Medications
☒ Previous Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☒ Medical Record Number
☒ Gender
☐ Integration Control Number (ICN)
☒Military History/Service Connection
☐ Next of Kin
☒ Other Unique Identifying Information (list below)

Education, Employment, Income, Utilization of VA Benefits and Services, Persisting Health Issues, Symptoms, Problem List, Diagnosis, Symptoms, Habits and Psychological/Mental Health, Labs, Images, Notes, Medications, Procedures, Patient Generated Health Data (e.g., wearable technology or connected devices) to record or monitor activity, Veteran Crisis Line Data, Cause of Death Data, Social Determinants of Health, Genomic and Biometric Data, Scanned Patient Records from Community Care, Claims and Payment Data, Rental Records Data.

PII Mapping of Components

Arches consists of multiple key components (databases). Each component has been analyzed to determine if any elements of that component collect Personally Identifiable Information (PII). The type of PII collected by Arches and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A					

1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information is being collected from already developed data sources within the CDW, including genomic data, community data; and patient generated data to include: Corporate Data Warehouse (CDW), Veterans Benefit Management System (VBMS) disability disability/compensation, VistA Imaging, OCC Patient Generated Health Data, Precision Oncology Research Database, USVets, Veterans Affairs/Department of Defense Identity Repository, Enlitic, Tablo, Expiration-of-Terms-of-Service Sponsorship Program (ETS-SP), Veteran Crisis Line/Suicide Prevention Data, Synthetic Patient Data, Agile MD eCART, Symphony AI/Ayasdi, TIBCO, VA Foresight, HyperScience, CCPI (Care and Payment Innovation), Box and stored in the Amazon Web Service (AWS) VAEC Cloud.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

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.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information is collected via secure SSL.

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

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.

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.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Data sources inputted into the Arches Platform will be authoritative sources of data. Data will be validated with informatics team to confirm no data corruption in submission. Further data validation will be completed as part of the set-up of the Arches platform, as outlined by the contract deliverables.

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

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

This question is related to privacy control AP-1, Authority to Collect

Title 38 of U.S. Code section 201. [38 CFR § 3.201 Exchange of evidence; Social Security and Department of Veterans Affairs - Code of Federal Regulations (ecfr.io)]

VHA Corporate Data Warehouse-VA (SORN 172VA10) https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf Authority for maintenance of the system: Title 38, United States Code, Section 501.

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.

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: The CDW (Corporate Data Warehouse) contains sensitive personal information – including social security numbers, names, and protected health information. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft may result.

Mitigation: VHA (Veterans Health Administration), facilities deploy extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of all employees and contractors. Security measures include access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance.

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.

The Arches project within the VHA will support direct patient care within the VHA and Veterans broadly for projects involving VBA and other governmental entities by providing a testing, development and validation environment for users that is securely housed within the VAEC.

Arches environment includes a Synthetic Data Generation Engine, including specific use cases below determined to be of high value for VHA. By adopting a cloud- based data analytics environment with a synthetic data engine, this project will provide on-demand access to understanding care pathways for direct patient care for any population of interest without the need for lengthy quality or IRB (Institutional Review Board) review, dramatically increasing the ability to use data to improve quality and operations for patient care.

Projects operating within the Arches environment clearly articulate and follow an approval process for data access; either bringing data into the environment or making use of data already provided within the environment. Projects make use of health record data, genomic data, social determinants of health data, and patient generated data for suicide prevention, chronic disease care pathway improvements, care coordination improvements, clinical care decision making improvements, administrative benefits processing improvements, operational efficiency improvements, and transition of care improvements. Projects include efforts to predict onset of clinical conditions and to improve care coordination or administrative processes related to care delivery or administrative processing of documents for Veteran care, benefits or operational efficiencies.

Clinical variation is a major contributor to suboptimal outcomes, increased cost and reduced Veteran satisfaction. Arches provides internal decision makers on-demand access to insights regarding variability in patient care clinical performance, including variability in best practices between providers and facilities. By understanding and reducing variation, decision makers can optimize improvements for direct patient care pathways.

With a nearly infinite number of ways for Veterans to be at risk for adverse health outcomes, understanding the direct patient care pathways for a specific population is of high value to the VHA. It is possible to create predictive models for disease progression, identify high risk Veterans and under treated Veterans and create Veteran lists which are used to support the direct patient care provided.

Despite the VHA's significant efforts, there are many Veterans with undiagnosed or under-treated conditions. These Veterans will have poor outcomes and lower quality of life. With Arches it is possible to mine the data and build algorithms to identify these Veterans and ultimately to develop optimized direct patient care pathways to serve Veterans.

Using Arches, the VHA creates knowledge and even specific algorithms and models which have value outside of the VHA to improve direct patient care. Arches provides a platform by which such outputs can be shared, and insights derived for Veterans within the VHA can support direct patient care for Veterans not served by the VHA.

Veteran Full Name: Name is used to identify Veterans and match data across different data sources
Last 4 of social security number: Last four is used as secondary identifier to match data
Date of Birth: Date of birth is used for analytics projects as age is often related to health outcomes
Phone number: phone number is an additional identifier that is part of the Corporate Data warehouse
Email: email is an additional identifier that is part of the Corporate Data Warehouse
Gender: Gender is used for analytics projects as gender systematically affects health outcomes
Race/Ethnicity: Race is used for analytics projects as race and ethnicity systematically affect health
Current Address: Current address is important for noting context of location, as location systematically affects health outcomes
Education: Education level is used for analytics projects as education systematically affects health outcomes
Employment: Employment is used for analytics projects as employment systematically affects health outcomes.
Income: Income is used for analytics projects as income systematically affects health outcomes
Utilization of VA Benefits and Services: Utilization is an important factor for analytics projects as health care utilization and utilization of resources affects health outcomes
Previous Medical Records: previous medical records are used in analytics projects to understand the longitudinal course of health and health concerns among service members
Persisting Health Issues: presenting health issues are important data points in understanding health care utilization and health outcomes
Problem List: problems lists are used in health analytics projects to understand health outcomes
Diagnosis: diagnoses are used in analytics projects to understand health outcomes
Symptoms: symptoms are used in analytics projects to better understand health concerns
Habits and Psychological/Mental Health: habits/behaviors and psychological and mental health are important data points to understand physical health and well-being and are used in data analytics projects to understand health outcomes
Labs: labs are important data elements for analytics projects as an objective biomarker of health and well-being
Images: images are important objective data elements for analytics projects to understand health outcomes
Notes: Notes are used in analytics projects to assess the documented language and understand health outcomes
Current Medications: Medications are used in analytics projects as important data elements to understand health outcomes
Procedures: procedures are used in analytics projects as important data elements to understand health outcomes

Patient Generated Health Data (e.g., wearable technology or connected devices) to record or monitor activity: PGHD is used in analytics projects to assess the impact or value of these data streams for understanding health and health outcomes
Military History/Service Connection: Military History/Service Connection is an important data elements for analytics projects to understand the historical context behind current health and wellness
Veteran Crisis Line Data: Veterans crisis line data is used to for analytics projects to continue to improve coordination of care and support for staff who are operating the crisis line
Cause of Death Data: Authoritative cause of death data is used for predictive modeling for health analytics projects
Social Determinants of Health: Social determinants of health data is used for data analytics projects as the context of a person's life systematically affects health outcomes
Genomic and Biometric Data: Genomic and biometric data are used for data analytics projects to evaluate the impact of those data sources on differential health outcomes
Scanned Patient Records from Community Care: Scanned patient records from community are used for analytics projects to develop improved processes for care coordination using technology
Claims and Payment Data: Claims and payment data are used for data analytics projects to evaluate the utilization of health care
Rental Records Data: rental records data are used in analytics projects as housing is known to systematically affects health outcome.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

Arches will allow for the evaluation of data, and creation of synthetic (artificial) datasets for quality improvement and operational purposes. The data generated is validated and assessed for privacy preserving properties and clinical utility. No data will be added to an individual medical record.

2.3 How is the information in the system secured?

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

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

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

There are procedures in place to guard PII/PHI. Users must provide documentation of authorization for PHI/PII for operational or research purposes prior to access provisioning. Access to PHI/PII is determined by the National Data Stewards (NDS) approval process for operational users and by Institutional Review Board (IRB) for research users.

There are technical safeguards to guard PHI/PII. No user can access Arches without permissions. All development, testing and validation occurs within the secure Arches environment within VAEC and operates under VAEC guidelines. Any data that is imported into the environment uses approved methods for data transfer; and any data that is exported outside the secure environment can do so only utilizing approved methods for data transfer as documented in the tables below.

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

Access to PII is determined by the currently assigned access level, contexts, and roles. The application manager is responsible for assigning users to the appropriate user roles to limit access for different parts of the application and assuring PII safeguards as documented in the user manual, technical manual, and system design document.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. <u>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.</u>

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

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

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

Access to PII is determined by the currently assigned access level, contexts, and roles. The application manager is responsible for assigning users to the appropriate user roles to limit access for different parts of the application and assuring PII safeguards as documented in the user manual, technical manual, and system design document.

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

Data will be stored in the VAEC (VA Enterprise Cloud). Arches is a platform in the VAEC. This includes: Corporate Data Warehouse (CDW), including genomic data, community data; and patient generated data to include the following sources: Corporate Data Warehouse (CDW), Veterans Benefit Management System (VBMS) disability/compensation, VistA Imaging, Office of Connected Care (OCC), Patient Generated Health Data (PGHD), Precision Oncology Research Database, USVets, Veterans Affairs/Department of Defense Identity Repository, Enlitic, Tablo, Expiration-of-Terms-of-Service Sponsorship Program (ETS-SP), Veteran Crisis Line/Suicide Prevention Data, Synthetic Patient Data, Agile MD eCART, Symphony AI/Ayasdi, TIBCO, VA Foresight, HyperScience, CCPI (Care and Payment Innovation), Box, and stored in the Amazon Web Service (AWS) VA Cloud.

PII/PHI includes: Veteran Full Name, Last 4 of social security number, Date of Birth, Gender, Race/Ethnicity, Current Address, E-mail Address, Personal Phone Number, Personal Email Address, Education, Employment, Income, Utilization of VA Benefits and Services, Previous Medical Records, Persisting Health Issues, Symptoms, Problem List, Diagnosis, Symptoms, Habits and Psychological/Mental Health, Labs, Images, Notes, Medications, Procedures, Patient Generated Health Data (e.g., wearable technology or connected devices) to record or monitor activity, Military History/Service Connection, Veteran Crisis Line Data, Cause of Death Data, Social Determinants of Health, Scanned Patient Records from Community Care, Claims and Payment Data, Rental Records Data.

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.

This question is related to privacy control DM-2, Data Retention and Disposal.

Information is maintained in accordance with General Records Schedule 20, item 4 which provides for deletion of data files when the agency determines that the files are no longer needed for administrative, legal, audit, or other operational purposes.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

Records are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States. The records are disposed of in accordance with General Records Schedule 20, item 4. Item 4 provides for deletion of data files when the agency determines that the files are no longer needed for administrative, legal, audit, or other operational purposes.

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

No paper records are involved with the Arches Platform; transitory data is only stored for the transaction time but after each transaction, data is purged from the cache.

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

In non-production environments, no PII or actual patient/user information is used. In production, PII is permanently stored, however the PII will not be part of the default data output; and will not be accessible outside of the VAEC. The synthetic generation system has the capability to output PII to specially authorized users for validation purposes within VAEC.

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.

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that the information contained in Arches 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: In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only as long as necessary.

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 shared/received with the Program Office or IT system***	***Describe the method of transmittal***
OIT/ Corporate Data Warehouse (CDW)	Analysis of CDW data, including synthetic data generation	Veteran Full Name, Last 4 of social security number, Date of Birth, Gender, Race/Ethnicity, Current Address, E-mail address, Phone Number, Education, Employment, Income, Problem List, Presenting Health Issues, Diagnosis, Symptoms, Habits, Psychological and Mental Health, Labs, Images, Notes, Medications, Procedures, Patient Generated Health Data, Military Service History, Social Determinants of Health, Genomic and Biometric Data	Secure SSL
Office of Information Technology (OIT)/ VistA Imaging	Analysis of imaging data, including synthetic data generation	Imaging Data	Secure SSL

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 shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Office of Connected Care (OCC)/ OCC Patient Generated Health Data (PGHD)	Analysis of PGHD data, including synthetic data generation	Patient Generated Health Data	Secure SSL
Office of Research and Development (ORD)/ Precision Oncology Research Database	Analysis of oncology data, including synthetic data generation	Genomic Data	Secure SSL
Office of Enterprise Integration (OEI)/ USVets	Analysis of data, including synthetic data generation	Veteran military history, demographics, socioeconomics, and utilization of VA benefits and services	Secure SSL
Office of Information Technology (OIT)/ Veterans Affairs/Department of Defense Identity Repository – VADIR	Analysis of data, including synthetic data generation	Demographic data, Military Service History	Secure SSL
Office of Information Technology (OIT)/ Enlitic	Analysis of data, including synthetic data generation	Radiologic Images (Magnetic Resonance Imaging (MRI), Computed Tomography (CT), X-ray	Secure SSL
Office of Information Technology (OIT)/ Tablo	Analysis of data, including synthetic data generation	Name, medical data from kidney dialysis machine	Secure SSL
Office of Information Technology (OIT)/ Expiration-of-Term-of-Service Sponsorship Program (ETS-SP)	Analysis of data, including synthetic data generation	Full Name, Last 4 of social security number, Date of Birth, Current Address, E-mail address, Phone Number, Education, Presenting Health Issues, Symptoms, Habits, and Psychological Health, and Military Service History	Secure SSL

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 shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Office of Information Technology (OIT)/ Synthetic Patient Data – MDClone	Analysis of data, including synthetic data generation	Full Name, Last 4 of social security number, Date of Birth, Current Address, E-mail address, Phone Number, Education, Employment, and Income, Presenting Health Issues, Symptoms, Habits, and Psychological Health, Military Service History, Genomic and Biometric Data, medical data from kidney dialysis machine, socioeconomics, and utilization of VA benefits and services, Patient Generated Health Data, completion data of activities related to reported mood, reported sleep, reported pain, and assessments, medical readings from glucose device, medical data from activities, heart rate and sleep, immunization records, Clinical care data, diagnoses, patient care team information, demographic data.	Secure SSL
Office of Mental Health and Suicide Prevention	Analysis of data including synthetic data generation	Name, mental health specific related data to include: Veterans Crisis Line Data, Cause of Death Data	Secure SSL

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 shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Office of Information Technology (OIT)/ Agile MD eCART	Analysis of data including synthetic data generation	Full Name, Last 4 of social security number, Date of Birth, Current Address, E-mail address, Phone Number, Education, Employment, and Income, Presenting Health Issues, Symptoms, Habits, and Psychological Health, Military Service History, Genomic and Biometric Data	Secure SSL
Office of Information Technology (OIT)/ Symphony AI/Ayasdi	Analysis of data including synthetic data generation	Full Name, Last 4 of social security number, Date of Birth, Current Address, E-mail address, Phone Number, Education, Employment, and Income, Presenting Health Issues, Symptoms, Habits, and Psychological Health, Military Service History, Genomic and Biometric Data	Secure SSL
Office of Information Technology (OIT)/ TIBCO	Analysis of data including synthetic data generation	Full Name, Last 4 of social security number, Date of Birth, Current Address, E-mail address, Phone Number, Education, Employment, and Income, Presenting Health Issues, Symptoms, Habits, and Psychological Health, Military Service History, Genomic and Biometric Data	Secure SSL

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 shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Office of Healthcare Innovation and Learning (OHIL)/ VA Foresight	Analysis of data including synthetic data generation	Full Name, Last 4 of social security number, Date of Birth, Current Address, E-mail address, Phone Number, Education, Employment, and Income, Presenting Health Issues, Symptoms, Habits, and Psychological Health, Military Service History, Genomic and Biometric Data	Secure SSL
Office of Information Technology (OIT)/ HyperScience	Analysis of data including synthetic data generation	Scanned patient records from community care including Full Name, Last 4 of social security number, Date of Birth, Current Address, E-mail address, Phone Number, Education, Employment, and Income, Presenting Health Issues, Symptoms, Habits, and Psychological Health, Military Service History, and imaging data	Secure SSL
Care and Payment Innovation (CCPI)/CCPI	Analysis of data including synthetic data generation	Scanned patient records from community care, claims and payment data including Full Name, Last 4 of social security number, Date of Birth, Current Address, E-mail address, Phone	Secure SSL

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 shared/received with the Program Office or IT system***	***Describe the method of transmittal***
		Number, Education, Employment, and Income, Presenting Health Issues, Symptoms, Habits, and Psychological Health, Military Service History, imaging data, and dental records data	
Office of Information Technology (OIT)/ Box	Analysis of data including synthetic data generation	Synthetic Data, De-identified Data related to heart health including presenting health issues, symptoms, habits, laboratory, and heart monitor values	Box secure file transfer.

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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

Follow the format below:
<u>Privacy Risk:</u> The sharing of data is necessary for the medical care of individuals eligible to receive care at a VHA facility. However, there is an unlikely risk that original data could be shared with an inappropriate VA organization or institution which would have a potentially catastrophic impact on privacy.

<u>Mitigation:</u> The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance.

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 shared/received 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***
NeuroScience	Operational quality improvement effort to better understand the value of biometric data to inform clinical care	Name, completion data of activities related to reported mood, reported sleep, reported pain, and assessments.	Veteran Owned Data that the Veteran authorizes to be shared via Terms of Service agreement between external organization and the Veteran	Secure Application Programming Interface (API), only accessible with a secure key. Access can be revoked by VA at any time.

BioStax	Operational quality improvement effort to better understand the value of Veteran initiated data to inform clinical care	Name, medical readings from glucose device	Veteran Owned Data that the Veteran authorizes to be shared via Terms of Service agreement between external organization and the Veteran	Secure Application Programming Interface (API), only accessible with a secure key. Access can be revoked by VA at any time.
NeuroFlow	Operational quality improvement effort to better understand the value of Veteran initiated data to inform clinical care	Name, wearable generated data (steps, heart rate, etc.), completion data of activities related to therapy (breathing, mindfulness activities, etc.), reported mood, reported sleep, reported pain, assessments, and journaling	Veteran Owned Data that the Veteran authorizes to be shared via Terms of Service agreement between external organization and the Veteran	Secure Application Programming Interface (API), only accessible with a secure key. Access can be revoked by VA at any time.
Podimetrics	Operational quality improvement effort to better understand the value of Veteran initiated data to inform clinical care	Name, images of foot from smart mat	Veteran Owned Data that the Veteran authorizes to be shared via Terms of Service agreement between external organization and the Veteran	Secure Application Programming Interface (API), only accessible with a secure key. Access can be revoked by VA at any time.
Abridge	Operational quality improvement effort to better understand the value of Veteran initiated data to inform clinical care	Name, recording and transcription from medical appointment	Veteran Owned Data that the Veteran authorizes to be shared via Terms of Service agreement between external organization and the Veteran	Secure Application Programming Interface (API), only accessible with a secure key. Access can be revoked by VA at any time.
Tablo/Outset	Operational quality improvement effort to better understand the value of Veteran	Name, medical data from kidney dialysis machine	Veteran Owned Data that the Veteran authorizes to be shared via Terms of Service	Secure Application Programming Interface (API), only accessible with

	initiated data to inform clinical care		agreement between external organization and the Veteran	a secure key. Access can be revoked by VA at any time.
Fitbit/Apple	Operational quality improvement effort to better understand the value of Veteran initiated data to inform clinical care	Name, medical data from activities, heart rate and sleep	Veteran Owned Data that the Veteran authorizes to be shared via Terms of Service agreement between external organization and the Veteran	Secure Application Programming Interface (API), only accessible with a secure key. Access can be revoked by VA at any time.
Simon/State Department of Health	Immunization records from state to improve quality of care	Name, immunization records	Business Associate Agreement (BAA), Interconnection Security Agreement (ISA)	Secure File Transfer
CareCentra	Operational quality improvement effort to better understand the value of individualized behavioral nudges to improve health outcomes	Clinical care data, diagnoses, patient care team information, demographic data, email, phone number	Veteran Owned Data that the Veteran authorizes to be shared via Terms of Service agreement between external organization and the Veteran	Secure Application Programming Interface (API), only accessible with a secure key. Access can be revoked by VA at any time.
Defense Health Agency Records/ Department of Defense	Military records to improve quality of care in transition for Veterans	Full Name, Patient Identifier, Date of Birth, Current Address, E-mail address, Phone Number, Education, Employment, and Income, Presenting Health Issues, Symptoms, Habits, and Psychological Health, Military Service History, Genomic and Biometric Data	Business Associate Agreement (BAA), Interconnection Security Agreement (ISA)	Secure File Transfer
Empallo	Empallo	Synthetic Data, De-identified Data related to heart health	Cooperative Research and Development	Secure File Transfer through Box

	Operational Quality improvement project to develop predictive algorithms for heart failure to improve health outcomes	including presenting health issues, symptoms, habits, laboratory, and heart monitor values	Agreement (CRADA)	
H2O.ai	H2O.ai, Inc. Operational Quality improvement project to test value of Artificial Intelligence (AI) models to predict surgery case duration and prolonged length of stay	Full Name, Last 4 of social security number, Date of Birth, Current Address, E-mail address, Phone Number, Education, Employment, and Income, Presenting Health Issues, Symptoms, Habits, and Psychological Health, Military Service History, Genomic and Biometric Data	Cooperative Research and Development Agreement (CRADA)	SSL
SynMRI	SyntheticMRI, Inc. Operational proof of concept to test the value of the SynMRI software to enhance MRI image quality for patient care	De-identified Imaging data	Cooperative Research and Development Agreement (CRADA)	PACS and network configuration supporting DICOM communication between PACS and computers running SyMRI

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: As appropriate to the connection, either a Veteran agreement or a BAA and MOU are in place to assure appropriate use of the data for Veteran care purposes. Access controls implemented and audit logs reviewed in concordance with ATO.

Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance.

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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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

The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. The NOPP is giving out when the Veteran enrolls or when updates are made to the NOPP copies are mailed to all VHA beneficiaries. Employees and contractors are required to review, sign, and abide by the National Rules of Behavior on an annual basis. https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

The relevant System of Record Notices (SORN) is 172VA10 VHA Corporate Data Warehouse-VA https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf.

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

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

The Veterans' Health Administration (VHA) facilities request only information necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information to the VHA, this will prevent them from obtaining the benefits necessary to them.

Employees and VA contractors are also required to provide the requested information to maintain employment or their contract with the VA

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

VHA permits individuals to agree to the collection of their personally identifiable information (PII) using paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA Notice of Privacy Practices and conversations with VHA employees. VA Forms are reviewed by (VHACO)Veterans Health Administration Central Office periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations were required. Where legally required VHA obtains signed, written authorizations from individuals prior to releasing, disclosing, or sharing PII and PHI. Individuals have a right to restrict the disclosure and use of their health information.

Individuals who want to restrict the use of their information should submit a written request to the facility Privacy Officer where they are receiving their care.

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.

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

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

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

Follow the format below:
<u>Privacy Risk:</u> There is a risk that an individual may not understand why their information is being collected or maintained about them.

<u>Mitigation:</u> This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries when there is a change in regulation. Employees and contractors are required to review, sign, and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online.

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?

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.

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).

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.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

There are several ways a Veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealtheVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at HTTPs://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office.

Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact Contract Officer Representative to obtain information upon request.

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 procedure for correcting inaccurate or erroneous information begins with a Veteran requesting the records in question from Release of Information (ROI). The Veteran then crosses out the information they feel is inaccurate or erroneous from the records and writing in what the Veteran believes to be accurate. The request for amendment and correction is sent to the facility Privacy Office for processing. The documents are then forwarded to the practitioner who entered the data by the facility Privacy Officer. The practitioner either grants or denies the request. The Veteran is notified of the decision via letter by the facility Privacy Officer.

Employees should contact their immediate supervisor and Human Resources to correct inaccurate or erroneous information. Contractors should contact Contract Officer Representative (COR) to correct inaccurate or erroneous information upon request.

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.

Veterans are informed of the amendment process by many resources to include the Notice of Privacy Practice (NOPP) which states:

> **Right to Request Amendment of Health Information.**
> You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.
> If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:
>
> • File an appeal

- File a “Statement of Disagreement”
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Information can also be obtained by contacting the facility ROI office.

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.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Veterans and individuals should use the formal redress procedures addressed above.

The procedure for correcting inaccurate or erroneous information begins with a Veteran requesting the records in question from Release of Information (ROI). The Veteran then crosses out the information they feel is inaccurate or erroneous from the records and writing in what the Veteran believes to be accurate. The request for amendment and correction is sent to the facility Privacy Office for processing. The documents are then forwarded to the practitioner who entered the data by the facility Privacy Officer. The practitioner either grants or denies the request. The Veteran is notified of the decision via letter by the facility Privacy Officer.

Employees should contact their immediate supervisor and Human Resources to correct inaccurate or erroneous information. Contractors should contact Contract Officer Representative (COR) to correct inaccurate or erroneous information upon request.

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.

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?

<u>*Principle of Individual Participation:*</u> *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:
<u>Privacy Risk:</u> There is a risk that a Veteran does not know how to obtain access to their records or how to request corrections to their records and that the health record could contain inaccurate information and subsequently effect the care the Veterans receive.

<u>Mitigation:</u> As discussed in question 7.3, the Notice of Privacy Practice (NOPP), which every patient receives when they enroll, discusses the process for requesting an amendment to one's records.

The VHA staffs Release of Information (ROI) offices at facilities to assist Veterans with obtaining access to their health l records and other records containing personal information.
The Veterans' Health Administration (VHA) established My HealtheVet program to provide Veterans remote access to their health records. The Veteran must enroll to obtain access to all the available features. In addition, Privacy and Release of Information Directive 1605.01 establishes procedures for Veterans to have their records amended where appropriate.

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?

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

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

VA employees must complete both the HIPAA and Information Security training. Specified access is granted based on the employee's functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information System Security Officer (ISSO), local area managers. Access is requested per policies utilizing Electronic Permission Access System (ePAS). Users submit access requests based on need to know and job duties. Supervisor, ISSO and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes. Once inside the system, individuals are authorized to access information on a need-to-know basis. Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle.

Access to computer rooms at facilities and regional data processing centers is generally limited by appropriate locking devices and restricted to authorized VA employees and vendor personnel. Information in the Synthetic Patient Generator may be accessed by authorized VA employees. Access to file information is controlled at two levels. The systems recognize authorized employees by series of individually unique passwords/codes as a part of each data message, and the employees are limited to only that information in the file which is needed in the performance of their official duties. Information that is downloaded from the Synthetic Patient Generator and maintained on laptops and other approved government equipment is afforded similar storage and access protections as the data that is maintained in the original files. Paper documents are similarly secured. Access to paper documents and information on automated storage media is limited to employees who have a need for the information in the performance of their official duties. Access to information stored on automated storage media is controlled by individually unique passwords/codes. An additional layer of information security consists of synthetic data output as default, unless PHI specifically required for an authorized user for an identified need.

Once inside the system, authorized individuals are allowed to access information on a need-to-know basis. Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle.

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.

Contracts are reviewed based on the contract guidelines by the appropriate contract authority (i.e., COR, Contracting Officer, Contract Review Committee).

Per specific contract guidelines, contractors can have access to the system only after completing mandatory information security and privacy training, VHA (HIPAA) Health Insurance Portability and Accountability training as well as the appropriate background investigation to include fingerprinting. Certification that this training has been completed by all contractors must be provided to the VHA employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must include in the contract clarification of the mandatory nature of the training and the potential penalties for violating patient privacy.

Contractors must have an approved ePAS request on file and access reviewed with the same requirements as VHA employees. As appropriate to the needs of the contract, contractors will complete a Business Associate Agreement (BAA) or Non-Disclosure Agreement (NDA) for review by the Office of General Council (OGC) and signed by all parties.

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

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

All VA employees who have access to VA computers must complete the onboarding and annual mandatory privacy and information security training. In addition, all employees who have access to Protected health information or access to VHA computer systems must complete the VHA mandated Privacy and HIPAA Focused raining. Finally, all new employees receive face-to-face training by the facility Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officer also perform subject specific trainings on an as needed basis.

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

If Yes, provide:

1. *The Security Plan Status is approved*
2. *The Security Plan Status Date, 03-June-2022*
3. *The Authorization Status is Authority to Operate (ATO)*
4. *The Authorization Date is 26-July-2022*
5. *The Authorization Termination Date 26-July-2023*
6. *The Risk Review Completion Date, 16-June 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.

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

An initial ATO was approved on 1/6/21, with subsequent ATOs approved. Most recent ATO approved until 08/12/23.

The FIPS 199 Classification of the system was Moderate.

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).

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.

The system is hosted on VAEC AWS. VAEC AWS EC has FedRAMP high authorization.

The system is Platform as a Service (PaaS).

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)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

We are operating within the VA Enterprise Cloud, not an external cloud system. All data is maintained within VA systems and owned by VA.

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

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

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

No ancillary data collected.

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

VA Accountability for security and privacy of VA data within VA Enterprise Cloud constraints. Contracts specify the need for rigorous attention to meet privacy and information security as part of the ATO process; and that the VA is responsible for ensuring requirements are met.

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

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

The system is not using RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Phillip Cauthers 255139 Digitally signed by Phillip Cauthers 255139
Date: 2022.12.28 12:55:23 -08'00'

Privacy Officer, Phillip Cauthers

LaWanda J. Wells 102840 Digitally signed by LaWanda J. Wells 102840
Date: 2023.01.02 11:44:03 -05'00'

Information System Security Officer, LaWanda Wells

Angela Gant-Curtis 105447 Digitally signed by Angela Gant-Curtis 105447
Date: 2022.12.28 15:07:22 -06'00'

Information System Owner, Angela Gant-Curtis

AMANDA L. PURNELL 227430 Digitally signed by AMANDA L. PURNELL 227430
Date: 2023.01.04 11:38:05 -05'00'

Project Manager, Amanda Purnell

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).

VA Notice of Privacy Practices: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

The relevant System of Record Notices (SORN) is 172VA10 VHA Corporate Data Warehouse-VA https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf.