Privacy Impact Assessment for the VA IT System called:

Advanced **P**atient **O**rac**L**e for **L**earning in **O**ncology

System Acronym: APOLLO

VA Salt Lake City

Veterans Health Administration

Date PIA submitted for review:

07/29/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Robert Janes	Robert.Janes@va.gov	801-582-1565 x1636
Information System Security Officer (ISSO)	Stuart E. Chase	Stuart.Chase@va.gov	410-340-2018
Information System Owner	Ahmad Halwani	Ahmad.Halwani@va.gov	801-560-9879

Abstract

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

Advanced Patient OracLe for Learning in Oncology. System Acronym: APOLLO aims to combine advanced informatics technology to address a critical knowledge gap regarding the suitability of different tele-oncology modalities to cancer patients by cancer diagnosis and phase of care. APOLLO is a general support system and analytical platform providing secure access to VA data and software in a high-performance computing environment (CSP FedRAMP Name: Microsoft – Azure Commercial Cloud, Microsoft – Azure Government) that are used to deliver content and applications to an audience made up of healthcare providers and partners across all VA medical centers and component facilities. APOLLO's mission is to improve the health of Veterans and enhance healthcare delivery in the Veterans Health Administration (VHA) facilitating the transfer of vital information to VHA providers and administrators.

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 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?*

Advanced Patient OracLe for Learning in Oncology (*APOLLO).* VA Salt Lake City is the VA Administration Office for this system. APOLLO will be hosted as Minor Application under Summit Data Platform (SDP). All APOLLO internal and external connections will be included in the SDP.

APOLLO is a general support system and analytical platform providing secure access to VA data and software in a high-performance computing environment (CSP FedRAMP Name: VA Enterprise Cloud Microsoft Azure Government High. Contract number: – GS-35-F-0884P VA118-17-F-1888) that are used to deliver content and applications to an audience made up of healthcare providers and partners across all VA medical centers and component facilities. APOLLO's mission is to improve the health of veterans and enhance health care delivery in the Veterans Health Administration (VHA) facilitating the transfer of vital information to VHA providers and administrators. The APOLLO system does not collect any information directly from individuals who are the subjects of the information. The APOLLO system does not connect, receive, or share PII/PHI with any other external (outside of VA) organization, IT system, third-party website, or application.

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial 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)

Additional information collected but not listed above:

- Dates of Care
- Dates of Diagnosis
- Date of death
- Private insurance status
- Laboratory results
- Medications and therapies
- Outpatient/inpatient clinic visits
- Pathology results
- Surgical procedure reports/records
- Radiographic imaging results
- ICD codes
- Disease-specific information
- Pertinent clinical/medical records
- Biometrics
- Health Information Benefits
- Claims Decision
- DD-214
- Financial Information

PII Mapping of Components

APOLLO connects only to its parent system Summit Data Platform (SDP). The type of PII processed by APOLLO and the reasons for the processing of the PII are in the table below.

PII Mapped to Components

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
Summit Data Platform (SDP)	Yes	Yes	• Name • SSN • Date of birth • Race/ethnicity • Gender	To ingest veteran cancer data into the APOLLO environment	• Role-based access granted through the Elevated

			• City of residence • County of residence • Zip code • Dates of care • Date of diagnosis • Date of death • Private insurance status • Laboratory results • Medications and therapies • Outpatient/inpatient clinic visits • Pathology results • Surgical procedure reports/records • Radiographic imaging results • ICD codes • Disease-specific information • Pertinent clinical/medical records • Biometrics • Health Information Benefits • Claims Decision • DD-214 • Phone Number • Email • Financial Information • Military History/service connection	for data reporting and analytics purposes, and clinical care decision making.	Privileges Access System (EPAS) • Data is encrypted at rest and in transit

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.

The Advanced Patient OracLe for Learning in Oncology APOLLO is a cloud data enterprise data management platform that aggregates cancer data from data sources available within Summit Data Platform (SDP).

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.

PII/PHI data are encrypted and transmitted through a secure network. SSNs are hidden from users and both SDP/APOLLO ensures that PII/PHI data is only released to authorized personnel. APOLLO will utilize the Azure Virtual Networks (VNETS), which wrap the system within MAG to encapsulate network access, allowing for connection to in-cloud and on-premises resources. Network security groups are implemented to restrict access to the service endpoints on these VNETs in Azure. Any VM disks used by APOLLO will be stored in Azure Storage Accounts and will be encrypted at rest. The APOLLO system will be backed up using the Azure Backup service and management activities on the cloud resources will be conducted through the Microsoft Azure Government portal for which PIV authentication is required. Access to APOLLO, will be restricted to select VA employees and no public access will be allowed. The only persons having access to the data will be persons authorized by the system owner. All persons having access to identifiable data will have completed the VA Privacy and HIPAA training and the VA Privacy and Information Security Awareness and Rules of Behavior training.

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.

APOLLO aims to combine advanced informatics technology to address a critical knowledge gap regarding the suitability of different tele-oncology modalities to cancer patients by cancer diagnosis and phase of care. The information collected will be used to conduct predictive analytics research with further data curation, algorithm development and applications of machine learning and AI techniques, analysis, and presentations. However, reports could be developed to assist the field in identifying problems with data content in authoritative sources that the field can then go to the authoritative sources to correct. Data consistency verification is performed in the Azure Data Factory (ADF) to ensure the data is not only successfully copied from source to destination, but also verified to be consistent between source and destination store. If inconsistent files are found during the data movement, the copy activity is aborted.

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 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."

The applicable legal authority falls under SORN:

VHA Corporate Data Warehouse - 172VA10/ 86 FR 72688
2021-27720.pdf (govinfo.gov)

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>
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:

<u>Principle of Purpose Specification:</u> 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.

Privacy Risk: The privacy risk is potential exposure of the limited data stored in this system. This system does not include the entire VA database but rather the partial data of the subset of research subjects whose information would be processed in the system at the time. There is a risk that data contained in the system may be shared with unauthorized individuals or that authorized individuals may share it with other unauthorized individuals.

Mitigation: VA security protocols are followed throughout the system. The APOLLO system is protected by a myriad of security features including limited, approved access, encryption, network isolation, 24-hour security monitoring, auditing, security configuration, scanning, patching, personnel security as well as physical security required by FISMA and continually undergoes FISMA standard evaluations and reviews.

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 information in this system is used to support VA sanctioned research to improve veteran's health through new and innovative processes and technologies.

- Name: Used as a patient identifier
- Social Security Number (SSN): Used as a patient identifier
- Date of Birth (DOB): Used to identify patient age and confirm patient identity
- Zip Code: Part of mailing address – uses for statistical analysis
- Current Medications: Used to identify and record current health and medical conditions, diagnosis, therapeutic procedures, clinical reports/tests, statistical reporting, modeling, prediction, and analysis.

- Previous Medical Records: Used to identify and record prior health and medical conditions, diagnosis, therapeutic procedures, clinical reports/tests, statistical reporting, modeling, prediction, and analysis.
- Race/Ethnicity: Used for statistical reporting, modeling, prediction, and analysis

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

Data sets are collected from database tables stored in Summit Data Platform (SDP). Database clients such as SQL Server Management Studio, software written in Java, Python, and R are used for this purpose. The analytic component uses the same set of software tools. Data produced: discerning pattern in data, visualization, and patterns. The effects of certain treatments. Prediction of outcomes in the future.

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?

APOLLO is hosted within the VA Enterprise Cloud Microsoft Azure Government High which is a general support system that provides a secure application and hosting environment for VA applications. APOLLO will be hosted by VA Enterprise Cloud, a cloud service provider that can support applications categorized up to High as rated in accordance with Federal Information Processing Standard (FIPS) 199. A dedicated private data link (Microsoft Express Route) provides all connectivity for VA resources communicating to the environment. Virtual Networks (VNets) wrap the applications within MAG to encapsulate network access. Access from the applications to VA internal resources such as Identity, Credential, and Access Management (ICAM) and Active Directory (AD) Services are conducted over the encrypted private data link to the VA Network. APOLLO will operate under the same level of security as other VA physical technology centers and supports existing VA security controls and certification requirements such as FISMA, HIPAA, HITECH, SAS-70, ISO 27001, FIPS 140-2 compliant end points, and PCI DSS.

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

The processing Social Security Numbers, personal individual information (PII) or personal health information (PHI), or VA Sensitive information will comply with appropriate VA policy. VA Controlled Cloud Computing Environment (VA3CE) accreditation boundaries allow for MS Azure Govt High to be leveraged as fully VA managed IT solutions. PII data are encrypted and transmitted through a secure network. The entire SSN is hidden from users, and SDP ensures that PII data is only released to the intended individual.

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

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

PII data are encrypted and transmitted through a secure network. APOLLO ensures that PII data is only released to the intended individual.

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.

The Office of Information and Technology (OIT) documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. This documentation and monitoring are performed using the Talent Management System (TMS). Access to the any system for research, testing or training is granted to VA clinical staffs and contractors by the local authority within each administrative area staff office. The only persons having access to the data will be persons authorized by the APOLLO system owner. All persons having access to identifiable data within the APOLLO system will have completed the VA Privacy and HIPAA training and the VA

Privacy and Information Security Awareness and Rules of Behavior training. Only VA accredited staff will have access to APOLLO data on a per protocol basis. All research activity is pre-approved by local privacy officer, research ISSO, and Institutional Review Board. This system uses FISMA standard processes for approving and monitoring access. This system is continually monitored and audited for compliance to FISMA security standards.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is retained by the system.
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

The following PII information is retained by the SDP system:

- Name
- Social Security Number (SSN)
- Mailing Address
- Personal Phone Number
- Personal Email Address
- Demographics
- Date of Birth (DOB)
- Data Interchange Personal Identifier (EDIPO)
- Usernames
- Biometrics

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.

Per the National Archives and Records Administration Request for Records Disposition Authority Records Schedule: DAA-GRS-2013-0005, Item 51, data is destroyed 5 years after the project/activity/transaction is completed or superseded, or the associated system is terminated, or

the associated data is migrated to a successor system, but longer retention is authorized if required for business us

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.

Yes. Veterans Health Administration Record Control Schedule (RCS) 10-1 (January 2020)
https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

Department of Veterans Affairs (VA), Office of Information & Technology RCS 005-1 (August 3, 2009) http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf and the General Records Schedule (http://www.archives.gov/records-mgmt/grs/).

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

SDP data will be deleted after decommissioning, following the Records Control Schedule (RCS 10-1), in compliance with VA policy, by physically deleting the stored data then overwriting the drives with generic/dummy data to ensure no previous ghost/residual data can be restored.

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

The Office of Information and Technology (OIT) documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. This documentation and monitoring are performed using Talent Management System (TMS). Access to the any system for research, testing or training is granted to VA clinical staffs and contractors by the local authority within each administrative area staff office.

De-identified or test data is used when feasible for test or initiation of users. In additional all access control policies and procedures are implemented in VAEC MAG to minimize the use of PII for testing, training, and research.

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.

Privacy Risk: Information is used for purpose of research. Only aggregate outcomes are reported as a result of research. There is no individual component that leaves the protected environment. When latter is the case, an elaborate de-identification process is conducted under review of the privacy officer and ISSO. The privacy risk is potential data breach, this possibility is higher if data retention of PII is longer.

Mitigation: There is no individual component that leaves the protected environment. When latter is the case, an elaborate de-identification process is conducted under review of the privacy officer and ISSO. To combat a data breach, SDP implements the same retention schedule as the source record. SDP relies on the data ingested from data sources. Old data are automatically archived based on retention schedule requirements.

SDP data will be deleted after decommissioning, following the Records Control Schedule (RCS 10-1), in compliance with VA policy, by physically deleting the stored data then overwriting the drives with generic/dummy data to ensure no previous ghost/residual data can be restored.

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***
Summit Data Platform (SDP)	Extracting phenomic information for individual patient conditions under investigation that will be used for statistical analysis, modeling, and prediction.	• SSN • Date of birth • Race/ethnicity • Gender • City of residence • County of residence • Zip code • Dates of care • Date of diagnosis • Date of death • Private insurance status • Laboratory results • Medications and therapies • Outpatient/inpatient clinic visits • Pathology results	VA internal secure network HTTPs and FIPS 140-2

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*
		• Surgical procedure reports/records • Radiographic imaging results • ICD codes • Disease-specific information • Pertinent clinical/medical records • Biometrics • Health Information Benefits • Claims Decision • DD-214 • Phone Number • Email • Financial Information • Military History/service connection	

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

Privacy Risk: There is a risk that information may be shared with unauthorized individuals or unauthorized programs or systems, in which the data could be further shared with unauthorized individuals, programs, or systems. The privacy risk is potential exposure of the limited data stored in this system. This system does not include the entire VA database but rather the partial data of the subset of research subjects whose information would be processed in the system at the time.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access controls and authorization are all measures that are utilized. The APOLLO system is protected by a myriad of security features including limited, approved access, encryption, network isolation, 24-hour security monitoring, auditing, security configuration, scanning, patching, personnel security as well as physical security required by FISMA and continually undergoes FISMA standard evaluations and reviews.

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***
N/A	N/A	N/A	N/A	N/A

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing
Privacy Risk: N/A

Mitigation: N/A

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 data stored in Summit Data Platform is received from sources such as CDW. Data is only collected for consented patients with approval of privacy. Notifications include the standard VA patient notification process notice of privacy practices as well as IRB approved consent forms and HIPAA authorizations (https://www.oprm.va.gov/privacy/systems_of_records.aspx). The applicable legal authority falls under SORN:

VHA Corporate Data Warehouse - 172VA10/ 86 FR 72688
2021-27720.pdf (govinfo.gov)

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

As outlined in VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their sensitive private information to VHA. The individual
shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

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

In addition to the Normal VA practices for Patient Privacy and Release Information, there may be additional research consent forms and practices that vary according to individual research protocols. These practices may be specific to individual research protocols, in which individuals may have the ability to consent or deny the use of their information.

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

<u>Privacy Risk:</u> There is a risk that members of the public may not know that the APOLLO system exists within the Department of Veterans Affairs. Additionally, there is a risk that veterans were not given notice their information was collected for use in APOLLO.

Mitigation: The VA mitigates this risk of not providing notice to the public in two ways, as discussed in detail in question 6.1 above, the PIA and SORN are published to notify and inform the public that information collected by the VA. Active participants in research studies are given notice and informed consent documents prior to their information being collected for the study.

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.

VHA Directive 1605.01 Privacy and Release Information', section 7(b) states the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Under the jurisdiction of VHA, VHA Directive 1605.01 'Privacy and Release Information', section 8 states the rights of the Veterans to amend to their records via submitting VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals seeking information concerning the existence of a record pertaining to themselves must submit a written request to the VA station of employment. Such request must contain a reasonable description of the records requested. In addition, identification of the individual requesting the information will be required in the written request and will consist of the requester's name, signature, address, and social security number, or another identifier, as a minimum. Individuals wishing to inquire whether this system of records contains information about them should submit a signed written request to the Manager, Medicare, and Medicaid Analysis Center, 100 Grandview Rd., Suite 114, Braintree, MA 02184. An individual who seeks access to records maintained under his or her name or other personal identifier may write the System Manager named above and specify the information being contested.

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.

Request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time, the System Manager for the concerned VHA

system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

7.5 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 considering 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?

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.

The Office of Information and Technology (OIT) documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. This documentation and monitoring are performed using the Talent Management System (TMS). Access to the any system for research, testing or training is granted to VA clinical staffs and contractors by the local authority within each administrative area staff office. The only persons having access to the data will be persons authorized by the system owner. All persons having access to identifiable data will have completed the VA Privacy and HIPAA training and the VA Privacy and Information Security Awareness and Rules of Behavior training. The security requirements and restrictions on the use of health information obtained from the Veterans Health Administration (VHA) in compliance with requirements of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, 45 CFR Parts 160 and 164.

Privacy Risk: There is a risk that information may be shared with unauthorized individuals or unauthorized programs or systems, in which the data could be further shared with unauthorized individuals, programs, or systems. The privacy risk is potential exposure of the limited data stored in this system. This system does not include the entire VA database but rather the partial data of the subset of research subjects whose information would be processed in the system at the time.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity.

Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access controls and authorization are all measures that are utilized. The APOLLO system is protected by a myriad of security features including limited, approved access, encryption, network isolation, 24-hour security monitoring, auditing, security configuration, scanning, patching, personnel security as well as physical security required by FISMA and continually undergoes FISMA standard evaluations and reviews.

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.

The only persons having access to the data will be the Information System Owner (ISO), and other persons as authorized by the ISO. Individuals will be granted access to the APOLLO system through the receipt of supervisor requests access from a system administrator. APOLLO will utilize the Azure Virtual Networks (VNETS), which wrap the system within VA Enterprise Cloud Microsoft Azure Government High to encapsulate network access, allowing for connection to in-cloud and on-premises resources. Network security groups are implemented to restrict access to the service endpoints on these VNETs in Azure. Any VM disks used by APOLLO will be stored in Azure Storage Accounts and will be encrypted at rest. OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring are performed using Talent Management System (TMS).

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.

Contractor access is verified through VA personnel before access is granted to any contractor. Contracts and contractor access are reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete non-disclosure agreements (NDA) as well as any pertinent role-based training prior to gaining system administrator access.

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 users with access to VA sensitive information or information system must complete VA Privacy and Security Awareness Rules of Behavior Training upon access and annually thereafter. Additionally, if users will be accessing protected health information (PHI) data VA HIPAA Privacy training must also be completed upon access, and additional training is required annually thereafter.

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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.***

APOLLO, previously known as ALCOVE, has not received an Authority to Operate (ATO). The system was registered in eMASS on December 9, 2020. eMASS System Name: AI COVID-CANCER (now APOLLO) - eMASS System ID# 1377. Summit Data Platform (SDP) has an ATO as

of April 8, 2022, with an expiration date of March 10, 2023. The FIPS 199 classification of SDP system is HIGH.

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.

APOLLO is a general support system and analytical platform providing secure access to VA data and software in a high-performance computing environment (CSP FedRAMP Name: VA Enterprise Cloud Microsoft Azure Government High. Contract number: – GS-35-F-0884P VA118-17-F-1888) that are used to deliver content and applications to an audience made up of healthcare providers and partners across all VA medical centers and component facilities. APOLLO's mission is to improve the health of veterans and enhance health care delivery in the Veterans Health Administration (VHA) facilitating the transfer of vital information to VHA providers and administrators. The FedRAMP process, as outlined in VA HANDBOOK 6517) is compliant with FISMA and is based on NIST Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

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.

Operating at a FedRAMP High Impact level, the VA Enterprise Cloud (VAEC), includes Microsoft Azure Government. The VAEC will maintain and operate in accordance with the application and VAEC service level agreements (SLAs), and APOLLO and it's parent system Summit Data Platform (SDP) will operate in its current environment in parallel as applicable. APOLLO will utilize VAEC General Support Services (GSS) when available and applicable to minimize cloud services costs and optimize operations. When the VA collects personal data from an individual, the VA will inform him or her of the intended uses of the

data, the disclosures that will be made, the authorities for the data's collection, and whether the collection is mandatory or voluntary. VA will collect no data subject to the Privacy Act unless a Privacy Act System of Records Notice has been published in the Federal Register and posted on the VA Systems of Records website. As such the VA will retain ownership rights over the data only for as long as necessary to fulfill the purposes for whit it is collected. These records will be destroyed in accordance with established VA records management principles.

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.

The VA Enterprise Cloud (VAEC) has established a series of contract vehicles to support the acquisition of cloud and the operation of the VAEC. VA Enterprise Cloud Microsoft Azure Government High, Contract number: – GS-35-F-0884P VA118-17-F-1888, is one of the approved acquisition vehicles available and for use to acquire cloud capacity. The VAEC is the hosting environment for all OI&T cloud applications, to ensure consistent utilization and execution in alignment with the VA Cloud Strategy. The ECSO, under the technical auspices of the Executive Director for Demand Management, is the governing authority for utilization of all VA cloud assets including but not limited to Microsoft Azure Government. All organizations, contracting teams, and program/project managers are expected to cooperate with the ECSO to ensure an orderly transition of governance of the current cloud-related aspects of their contracts to the ECSO.

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.

The VA Enterprise Cloud (VAEC) is a multi-vendor platform for the development and deployment of VA cloud applications. APOLLO will be hosted by the VAEC within the VA Enterprise Cloud Microsoft Azure Government High. Contract number: – GS-35-F-0884P VA118-17-F-1888. The VAEC also provides a set of common services such as

authentication and performance monitoring, speeding, and simplifying the development of new applications in or migration of existing applications to the cloud. In accordance with the Cloud Policy Memorandum dated October 29, 2019, APOLLO project managers and business owners will ensure that all efforts comply with IT security, privacy, and networking requirements.

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).

Robotic Process Automation (RPA) or bots will not be utilized in the APOLLO system.

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.

Robert R. Janes 252253

Digitally signed by Robert R. Janes 252253
Date: 2022.08.09 08:14:55 -06'00'

Privacy Officer, Robert Janes

Stuart E. Chase 3385791

Digitally signed by Stuart E. Chase 3385791
Date: 2022.08.09 11:07:57 -04'00'

Information Systems Security Officer, Stuart E. Chase

Ahmad S Halwani 582833

Digitally signed by Ahmad S Halwani 582833
Date: 2022.08.09 09:12:40 -06'00'

Information Systems Owner, Ahmad Halwani

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).

The applicable legal authority falls under SORN: VHA Corporate Data Warehouse - 172VA10/ 86 FR 72688 2021-27720.pdf (govinfo.gov)

The weblink: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3147