Privacy Impact Assessment for the VA IT System called:

Prospect

VHA

Office of Research & Development (ORD)

Date PIA submitted for review:

09/08/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kimberley E Murphy	Kimberley.Murphy@va.gov	(781) 331-3206
Information System Security Officer (ISSO)	Stuart Chase	Stuart.chase@va.gov	(410) 340-2018
Information System Owner	Siamack Ayandeh	Siamack.Ayandeh@va.gov	(978) 257-2714

Abstract

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

Prospect system is an enclave in Amazon Web Services (AWS) VA Enterprise Cloud (VAEC) used for conducting research and training that consists of different types of instances, machine images, storage, and platform software. The system stores patient health data that is analyzed using VA approved software and custom code and is accessed via secure servers and privileged and non-privileged two factor authenticated accounts. The system is managed and used by VA staff from the VA network. Prospect consists of a number of subnets in VA Enterprise Cloud development Virtual Private Cloud (VPC) and is protected by AWS-Cloud Service Provider and VAEC AWS GOV Cloud FISMA High security mechanisms.

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?*

VA Enterprise Cloud Prospect is infrastructure, an enclave and a single site, in AWS VA Enterprise Cloud for conducting research projects defined by an active protocol and under oversight of an Institutional Review Board (IRB), needing access to VA Enterprise Cloud (VAEC) elastic resources, model of operations, and utility payment model using the Veterans Health Administration's Office of Research and Development (ORD) funding Resources.

The system is owned, operated, and controlled by VA Office of Research and Development (ORD). Prospect is used for analytics and performing scientific computations that help advance our state of knowledge with regards to a variety of diseases which impact veterans, and the population by extension.
Example of cloud resources include: -Amazon Elastic Compute (EC2) instances, - Storage services such as simple storage service (s3) and Glacier, -Platform software such as Relational Data Base Service (RDS) for cataloging of data, -and other approved cloud capabilities and common VAEC services for Authentication, Authorization, and Accounting (AAA), patching, backup, monitoring, and similar.
Prospect would be home to hundreds of research study marts. Each study mart would have several users.
A study mart consists of two components: First is a data component and second is a research application component. A Research Data Repository (RDR) component contains the data (PHI/PII) and the analytic component are the applications which use the Research Data Repository.
Research Data Repository receives, curates, and if needed de-identifies phenomics, multi-omics, and imaging data used by analytic components. Sources of data include other systems in VA or partner institutions such as: Central Data Warehouse (CDW), Electronic Data Warehouse (EDW), VA Informatic and Computing Infrastructure (VINCI), GENISIS, on-prem and similar VA sources via VA network and VA Trusted Internet Connection (TIC), 3rd party vendors and partners via the network or Cloud Service Provider. Prospect connects to these systems to transfer the study data which is used further for analytics.
Applications and platform software for above receive and store the data, enable correlated multi-omics search and view, perform Natural Language Processing (NLP) to extract or de-identify the data, and curate the data for analysis and reporting. Analytic Applications conduct predictive analytics research with further data curation, algorithm development and applications of machine learning and Artificial Intelligence (AI) techniques, analysis and presentation exemplified by various protocols, associated imaging analysis pipeline applied to various imaging modalities. De-identification consists of removing all PII associated with a record. This may include all 18 fields identified by HIPAA such as: names, addresses, SSN, dates of visits, etc. which are protected personal information. Only patient identifiers are used to identify a record and a cross walk is maintained within the VA firewall to associate the patient identifier with the PII. The process and software for this de-identification has been in operation within VA for 4 years with no known incidents. The magnitude of harm is not the entire VA database but rather the partial data of the subset of research subjects whose information would be currently being processed in the system at the time. Such an event has potential to negatively impact the VA's reputation and reduce the public's trust in protecting its information.
Prospect has an Authority to Operate (ATO) from VA OI&T Development Security & Operations which is reviewed and extended periodically.
Completion of this PIA does not impact any processes or technology in Prospect nor any revisions of a SORN is required.
The authority for the system is Veterans' Benefits: Functions of Veterans Health Administration, 38 U.S. Code § 7303. As stated in Privacy Act Systems of Record Notice (SORN) 34VA12, "Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA", Title 38, United States Code, Section 501 is the authority for maintenance and operation of this 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, 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)

Add Additional Information Collected But Not Listed Above Here

- PII and PHI as held in CDW tables.
- PatientLabChem for test results
- CPRSOrder for various procedures
- BCMADispensedDrug for drugs prescribed

- RxOutpat for outpatient visits
- Surgery for various procedures
- Patient for identifying the person
- Actionable Mutations for genomic basis of treatments
- ICD9/10 code table for codifying conditions and treatments
- Oncology Raw for data files returned from analysis of patient's genome
- Outpat for outpatient visits
- OMOP for a global standard vocabulary of medial terms and conditions
- Imaging data from various imaging modalities
- Web URL
- Photographic image - Photographic images are not limited to images of the face
- Finger or voice print
- Device identifiers and serial number
- Genomics: FASTQ, Variant Call Format (VCF) formatted files

PII Mapping of Components

Prospect consists of 2 key components. A Research data repository (RDR) or study data, and a analytic study mart where the data is analyzed. Each component has been analyzed to determine collected PII and the data sources from which the data is collected. The type of PII collected by Prospect and the reasons for the collection 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
Central Data Warehouse (CDW) and syndicated Cerner data (EDW) VA Informatics and Computing Infrastructure (VINCI) Replica (pull to RDR)	No	Yes	Name, SSN, DoB, Medical Records, Race/Ethnicity, and other as listed in section 1.1	Medical Research using Lab results, orders of medication, Records of outpatient visits, Surgery records, Patient personal information, Actionable genetic profile, international codes used to identify disease, etc.	Access control, encryption, network isolation, 24 hour security monitoring, auditing, security configuration, scanning, patching, personnel security (MFA) as well as physical security and other FISMA requirements.
Genomic Information System for Integrated Science (Genisis) Research DB and	Yes	Only patient coded data is stored	Only patient coded data is stored	Medical Research using raw genomics results files, variant calling results, results of secondary analysis	Access control, encryption, network isolation, 24 hour security monitoring, auditing, security configuration, scanning, patching, personnel

PoP-Research-DB (pull to RDR)					security (MFA) as well as physical security and other FISMA requirements.
Vista Imaging (pull to RDR)	Yes	Yes	Name, DoB, Medical Records, Race/Ethnicity, and other as listed in section 1.1	Medical Research using Vista imaging data such as Computed Tomography (CT), Pathology slides, MRI	Access control, encryption, network isolation, 24 hour security monitoring, auditing, security configuration, scanning, patching, personnel security (MFA) as well as physical security and other FISMA requirements.
The VA Information Resource Center (VIReC) Center for Medicare and Medical Services (CMS) Database (pull to RDR)	No	Yes	Name, SSN, DoB, Medical Records, Race/Ethnicity, and other as listed in section 1.1	Medical Research using Clinical Records	Access control, encryption, network isolation, 24 hour security monitoring, auditing, security configuration, scanning, patching, personnel security (MFA) as well as physical security and other FISMA requirements.
VIREC Morbidity Data Repository (VBA) database (pull to RDR)	No	Yes	Name, SSN, DoB, Medical Records, Race/Ethnicity, and other as listed in section 1.1	Medical Research using Dates of events	Access control, encryption, network isolation, 24 hour security monitoring, auditing, security configuration, scanning, patching, personnel security (MFA) as well as physical security and other FISMA requirements.
VHA OI&T Local database (pull to RDR)	No	Yes	Name, SSN, DoB, Medical Records, Race/Ethnicity, and other as listed in section 1.1	Medical Research using EHR structured data sets, raw genomic files returned from vendors, imaging files for various modalities, study database extracts	Access control, encryption, network isolation, 24 hour security monitoring, auditing, security configuration, scanning, patching, personnel security (MFA) as well as physical security and other FISMA requirements.

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.

A study in Prospect transfers information from the primary and secondary data sources listed below to its data repository in order to conduct data curation and analytics.

Central Data Warehouse (CDW) is a VA wide secondary data source

Electronic Data Warehouse (EDW) is a VA wide secondary data source

VA Informatic and Computing Infrastructure (VINCI) is a research enclave that has access to CDW for creation of study databases.

GENISIS stores genomics information

3rd Party vendors e.g. genomics result files from Natera for VA patients

Other sources within VA such as Centers for Medicare and Medicaid Services (CMS) to verify the date of death

VISTA CPRS and similar for collection of imaging data. VISTA is the VA electronic health record system and is a primary data source

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 extracted as electronic transmission from primary and secondary data sources and systems listed in section 1.2, e.g. databases such as Central Data Warehouse which in turn extracts information from VISTA and CERNER EHR. Information is extracted using a database client, stored on a server and then transferred to the Prospect study space. Result files from genomic vendors such as Natera are returned via electronic means for storage in VA Enterprise Cloud. No paper-work is involved.

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.

Information is checked at the primary source Electronic Health Record (EHR) system where it is collected that it falls within acceptable range and is accurate.
It is further checked when data is transferred to a central data warehouse (secondary data source) for wider use and dissemination by business information line group within VA.
Finally, data is checked by researchers when used for modeling and analysis in PROSPECT to ensure that data falls within acceptable ranges and outliers are removed from the data set.

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 authority for the system is Veterans' Benefits: Functions of Veterans Health Administration, 38 U.S. Code § 7303, which states, in part:
(a)(1) In order to carry out more effectively the primary function of the Administration and in order to contribute to the Nation's knowledge about disease and disability, the Secretary shall carry out a program of medical research in connection with the provision of medical care and treatment to veterans. Funds appropriated to carry out this section shall remain available until expended.
(2) Such program of medical research shall include biomedical research, mental illness research, prosthetic and other rehabilitative research, and health-care-services research.
The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule permits the use of protected health information for research purposes pursuant to a HIPAA authorization, which is obtained from individual patients under the MVP research study to access, collect and store their health information and blood sample(s) for future research use.

As stated in Privacy Act Systems of Record Notice (SORN) 34VA12, "Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA", Title 38, United States Code, Section 501 is the authority for maintenance and operation of this system.

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: PHI is collected for the purpose of research to improve the care of the veterans and the general population by extension. Only data relevant to the primary purpose of the research, defined in a protocol, and overseen by an IRB is collected. Information is collected from primary and secondary data sources within VA.
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 is currently being processed in the system at the time.

Mitigation: VA security protocols are followed throughout the system. The VAEC is a FISMA High environment and approved by VA to hold PII and PHI. This system is protected by a myriad of security features including but not limited to 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
- SSN: Used as a patient identifier
- DoB: Used to identify patient age and confirm patient identity
- Current Medications: Input for modeling and prediction
- Previous Medical Records: Input for modeling and prediction
- Race/Ethnicity: Input for modeling and prediction
- Other PII listed in section-1.1: is part of the person's table and may be used to uniquely identify the patient over time as patient coordinates change
- Medications and medical records: are used to create a cohort of patients which are the focus of a study for a specific disease and analysis of effect of drugs and various treatments
- PatientLabChem: for test results
- CPRSOrder: for various procedures
- BCMA_Dispensed_Drug: for drugs prescribed
- RxOutpat: for outpatient visits data
- Surgery: for various procedures
- Patient: for identifying the person
- Actionable Mutations: for genomic basis of treatments
- ICD9/10 code: table for codifying conditions and treatments
- Oncology Raw: for data files returned from analysis of patient's genome
- Outpat: for outpatient visits data
- OMOP: for a global standard vocabulary of medial terms and conditions
- Imaging data: from various imaging modalities to analyze health conditions
- Web URL: to identify patients
- Device identifiers and serial number: to calibrate data
- Genomics: FASTQ, Variant Call Format (VCF) formatted files: contain data for genomic basis of disease and treatments

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 such as CDW. Database clients such as SQL Server Management Studio, software written in Java, Python, and R are used for this purpose. Imaging related software such as POSDA may be used. The analytic component uses the same set of software tools. Data produced: discerning pattern in data, visualization of 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?

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?

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

Data is encrypted using VA approved standards both at rest and in motion. Secure transmission protocols are used for moving the data within the VA Intranet which is protected by Federal Government mandated Trusted Inter Connection (TIC) technology. When possible SSN are replaced by patient identifiers. A Prospect Rules of Behavior document is reviewed and signed by users. Only VA accredited staff have access to VAEC-Prospect and data on a per protocol basis. List of approved personnel is maintained in DART and similar systems on perm. An IRB has oversight for each protocol. All research activity is pre-approved by local privacy officer and research ISSO. This system uses FISMA standard processes for approving and monitoring access. This system is continually monitored and audited for compliance to FISMA security standards.

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. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Add answer here:

VAEC-Prospect study marts import data from study databases which have collected the data from primary and secondary data sources. Latter occurs under control and auspices of National Data System (NDS), Business Information System Line (BISL), and various ORD mechanisms such as an IRB and central IRB. Such controls require extensive training and credentialing of VA research staff who handle PHI/PII. Latter is a requirement of adding staff to the list of approved staff in a protocol as well as manager approval. Only such VA accredited staff have access to instances in the VAEC and data on a per protocol basis. List of approved personnel is maintained in DART system on perm. An IRB has oversight for each protocol. All research activity is pre-approved by local privacy officer and research ISSO.

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

A copy of information is retained as is required by VA and for use in potential future analysis. Name, SSN, DoB, Current Medications, Previous Medical Records, Race/Ethnicity are stored

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 stored indefinitely. Active analysis usually takes a few years and is often gated by growing the number of participants in the research project. The data is then archived to reduce the cost of storage for possible future reference.

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.

When managing and maintaining VA data and records, PROSPECT follows the guidelines established in the NARA-approved Department of Veterans Affairs (VA), Veterans Health Administration Record Control Schedule (RCS) 10-1 (March 2011) 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

The records contained in this system are only copies of records kept in primary and secondary data sources as well as study databases elsewhere. No records have not been scheduled currently and will be kept indefinitely until such time as they are no longer needed. The records may not be destroyed until VA obtains an approved records disposition authority from the Archivist of the United States. Records will be destroyed according to VA Handbook 6500.1 & NIST Special Publication 800-88.

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

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 is performed through the use of 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.

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: 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, and if outside of VA network, an elaborate de-identification process is

conducted under review of the privacy officer and ISSO. 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 study data of the subset of research subjects whose information is currently being processed in the system at the time.

Mitigation: There is no individua l 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 environment where information is held and processed is protected by both OI&T and the VA Enterprise Cloud security mechanisms. Furthermore, the enclave went through a comprehensive process to get an ATO (valid till March 2023) and will be monitored for maintaining security standards. This 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 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VHA ORD	VA Informatics and Computing Infrastructure (VINCI)	Structured Query Language (SQL) files and data for EHR, phenomics data sets	Transport Layer Security, SMB, or AWS CLI, encrypted hard drives
VHA MVP	Genomic Information System for Integrated Science (Genisis) High Performance Compute Cluster (HPC) and PoP-Research	Raw genomics results files, variant calling and other secondary analysis results, Phenomics data sets	Transport Layer Security, SMB, or AWS CLI, encrypted hard drives
VHA OI&T	VISTA	Computed Tomography (CT) scans, Pathology slides, System Log files, sample clinical data that may contain Protected Health Information (PHI)	Hypertext Transport Protocol Secure (HTTPs), Webdav, Picture Archiving and Communication System (PACS), Electronically pulled from VistA through Computerized Patient Record System (CPRS)
The VA Information Resource Center (VIReC)	VBA, VBMS	Social Security Number, Benefits Information, Claims Decision, DD-214, dates of events	Compensation and Pension Record Interchange (CAPRI) electronic software package
The VA Information Resource Center (VIReC)	Center for Medicare and Medical Services (CMS) Data	Clinical Records	Transport Layer Security, SMB, or AWS CLI
VHA OI&T	Local Server in 10.0.0.0/8 domain, Hard Drives from vendors	Study database extracts, Genomics raw data, imaging, Genomic results file with various formats	Transport Layer Security, SMB, or AWS CLI, Hypertext Transport Protocol Secure (HTTPs), Webdav, encrypted HD

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.

Follow the format below:
Privacy Risk: There is a risk that information may be shared with unauthorized VA program or system or that data could be shared. 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 currently being 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. This 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 processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Open Data Common Consortium (University of Chicago)	To send De-identified Phenomics, Imaging Data, Patients Genes data from VA	De-identified Phenomics, Imaging Data, Patients Genes data	Data Use Agreement	Secure Network connection including s3 transfer and shipping of encrypted hard drives containing de-identified data (no PII)
Natera NCI & DoD	Receiving of genomics results files	Genomics files in VCF format	Data Use Agreement	Secure Network connection including s3 transfer
Department of Energy National Labs	To send De-identified Phenomics, Imaging Data, Patients	De-identified Phenomics, Imaging Data, Patients Genes data	Data Use Agreement	Secure Network connection, s3 transfer, encrypted hard drives

	Genes data from VA			
APOLLO DoD/NCI	Receiving of genomics data files and associated phenomics data sets from DoD & NCI	Precision oncology, raw genomic data, phenomics, imaging data	Data Use Agreement	Secure network connection, s3 transfer, encrypted hard drives

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:
Privacy Risk: Imperfections in the de-identification process. Attempts to potential to re-identify the patient using tools that could assist in identifying patients.

Mitigation: Data transfers are over encrypted secured connections and use specific access rights agreed to by both parties defined in a DUA. Risks are mitigated due to data being deidentified prior to external sharing. VA are de-identified and shared with a known partner and using a DUA. The partner stores information in a FISMA moderate environment and VA remains the data steward. Risks are mitigated due to data being deidentified prior to external sharing.

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.

We get data from primary sources such as VISTA and secondar data 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.va.gov/vhapublications/ViewPublication.asp?pub_ID=3147

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

Yes, in addition to the normal VA standard opportunities and right to decline offered to all patients, only consents are returned and there is no penalty for research protocols.
Normal VA practices of "Notice of Privacy Practices" and HIPAA waver

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 standard processes for right to consent additional research consent forms vary with protocol and are protocol specific. The use is for purpose of research and the defined protocol. Normal VA practices of "Notice of Privacy Practices" and HIPAA waiver. Individuals do not have the right to consent to particular uses of the information.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

Principle of Transparency: Has sufficient notice been provided to the individual?

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

Follow the format below:
Privacy Risk: Sufficient notice is always provided, if there is no consent then there is no data collection. Consent is continually reevaluated in every new protocol review and is approved by the associated VA IRB team, privacy officer and information systems security officer.

Mitigation: Each protocol stores data in such a way that only approved research team has permissions to access the data. Continual evaluation of consents are done with each new protocol approved

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.

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

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
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 period, the System Manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

7.5 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?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:
Privacy Risk: N/A
As pointed out in sections 1.1 and 7.1, Prospect does not collect any PII/PHI directly from patients, only from primary and secondary data sources. Therefore, any queries by individuals and associated process and redress is handled at VHA level. Per section 1.1 Prospect deploys VA wide standards to controlling access and the risk has been accessed as being low to moderate.

Mitigation: N/A
Any mitigation processes are VHA wide per section 7.1. Any mitigation action may impact the primary data sources, and through updates may impact Prospect.

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.

Access is defined in the protocol and list of people with access are defined. To gain access to Prospect, the user's supervisor requests access from a system administrator. The application is behind the VA firewall and is accessible only to VA staff. Any change is approved by an Institutional Review Board (IRB)

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.

VA Contractor access is verified through VA personnel before access is granted to any VA 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 additional 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.

Prior to receiving access, the user must complete and sign User Access Request Form. The user must complete, acknowledge, and sign that he/she will abide by the VA Rules of Behavior. The users must complete annual mandatory security and privacy awareness and HIPAA training.

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.***

Yes, System Security Plan Date – 08/03/2022. PROSPECT (System ID 1091) received a one year ATO on 03/10/2022. The Authorization Status for PROSPECT is Authorization to Operate (ATO) and was authorized on 3/10/2022. The Authorization Termination Date is 03/10/2022.

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.

PROSPECT is hosted within the VA Enterprise Cloud (VAEC) and the service model is Infrastructure as a Service (IaaS).

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.

N/A

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

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

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

N/A

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

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

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

N/A

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

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

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Digitally signed by Kimberly E. Murphy 183320
Date: 2022.10.12 08:31:40 -04'00'

Privacy Officer, Kimberley E Murphy

Stuart E. Chase 3385791

Digitally signed by Stuart E. Chase 3385791
Date: 2022.10.12 10:49:05 -04'00'

Information System Security Officer, Stuart Chase

SIAMACK AYANDEH

Digitally signed by SIAMACK AYANDEH
Date: 2022.10.12 11:12:41 -04'00'

Information System Owner, Siamack Ayandeh

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).