Privacy Impact Assessment for the VA IT System called:

Research and Analytical Science Platform (RASP) Azure

Veterans Health Administration

Infrastructure Operations – Application Cloud Edge Services – Enterprise Cloud Solutions Office (IO-ACES-ECSO)

Date PIA submitted for review:

6/13/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kimberly Murphy	Kimberly.murphy@va.gov	781-331-3206
Information System Security Officer (ISSO)	Albert Estacio	Albert.Estacio@va.gov	909-583-6309
Information System Owner	Christopher Cardella	Christopher.cardella@va.gov	512-983-5911 512-590-9414

Abstract

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

The Enterprise Cloud Solutions Office (ECSO) in the Infrastructure Operations (IO) has developed the VA Enterprise Cloud (VAEC), Research and Analytical Science Platform (RASP) Azure, which will host all suitable VA cloud Environmental research projects / applications in the cloud. Use of the VAEC is required based on the VA Cloud Policy memo jointly issued by the OIT's Demand Management and Strategic Sourcing offices. Sponsor Organization: Office of Information and Technology. RASP Azure is a platform for protocol-based research projects where each protocol is under auspices of an Institutional Review Board (IRB) or other delegate and follows the VA Central IRB Standard Operating Procedures (SoP) for conduct of research including study data collection, handling, usage, and analysis. RASP Azure consists of two components: (1) Data component: A Research Data Repository (RDR) contains the data which receives and curates data. Sources of data include study databases which have extracted data from researcher- and analyst-directed file shares and tables and (2) Stand-Alone Applications: RASP Azure supports stand-alone applications with application teams that bring their own data.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

The VA-owned Research and Analytical Science Platform (RASP) Azure will host all suitable VA research projects / applications in the cloud and provide services to enable researchers to perform work studies in a dedicated and secure location.

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

The business purpose of the Research and Analytical Science Platform (RASP) Azure is to provide VA Researchers modernized, maintained infrastructure and tools specific to needs of data researchers who need such resources successfully and efficiently perform research-based projects both large and small in in a scalable environment. This program aims to provide VA researchers modernized tools and services to allow more time to dedicate to research rather than securing IT resources and maintaining services outside their area of specialization while leveraging tools and services made available by industry leading cloud platform providers to better improve Veteran experiences.

C. Indicate the ownership or control of the IT system or project.

The RASP Azure Platform is VA owned and VA operated.

2. Information Collection and Sharing

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

Research data can include thousands/millions of individual data records and will be determined by the size of the research project data studies.

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

Veteran data is utilized by VA Research teams to perform various research studies to improve veteran care.

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

Information sharing will be conducted with researcher- and analyst-directed file shares and tables and temporary individual tenants built for individual research projects, both of which will house PII/PHI data. Specific PII/PHI data elements will vary based on research being performed. At this time, PII/PHI data cannot be identified as this will be researcher and analyst-directed.

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.

The RASP Azure platform is cloud-based and therefore not operated from multiple sites.

3. Legal Authority and SORN

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

Title 38 USC 7301 and 34VA10- Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

As stated in System of Record Notice (SORN) 34VA10 Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA. The procedure outlined in the SORN complies with VHA Directive 1605.01, Paragraph 7 and VA Regulation 38 CFR § 1.577.

https://www.govinfo.gov/content/pkg/FR-2021-06-23/pdf/2021-13141.pdf

D. System Changes

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

Existing processes do not apply as this is a new platform service supporting research-based projects.

K. Whether the completion of this PIA could potentially result in technology changes

Existing technology changes do not apply as this is a new platform service supporting research-based projects.

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☒ Personal Fax Number
☒ Personal Email Address
☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☒ Health Insurance Beneficiary Numbers Account numbers
☒ Certificate/License numbers*
☒ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number

☒ Medical Record Number	☒Military History/Service Connection
☒ Gender	☐ Next of Kin
☐ Integrated Control Number (ICN)	☒ Other Data Elements (list below)

May include all 18 fields identified by Health Insurance Portability and Accountability Act (HIPAA) regulation such as: names, addresses, Social Security Number (SSN), dates of visits, etc. which are protected personal information:

Name

• Address (all geographic subdivisions smaller than state, including street address, city county, and zip code)

• All elements of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)

•Personally Identifiable Information (PII) and Protected Health Information (PHI) as held in researcher- and analyst-directed file shares and tables.

•Phenomics from Central Data Warehouse (CDW) and similar sources; domains include:

• PatientLabChem for test results

• Computerized Patient Record System (CPRS) Order for various procedures

• Bar Code Medication Administration (BCMA) DispensedDrug for drugs prescribed

• RxOutpat for outpatient visits

• Surgery for various procedures

• PatientID for identifying the person receiving treatment

• Surgery for various procedures

• Actionable Mutations for genomic basis of treatments

• International Classification of Disease (ICD) 9/10 code table for codifying conditions and treatments

• Oncology Raw for data files returned from analysis of patient's genome

• Output for outpatient visits

• Observational Medical Outcomes Partnership (OMOP) for a global standard vocabulary of medial terms and conditions

• Genomics: FASTQ, Variant Call Format (VCF) formatted files

• All data coming from commercial Picture Archiving and Communication System (PACS) and other medical devices including but not limited to Digital Imaging and Communications in Medicine (DICOM) files

• Web Uniform Resource Locator (URL)

• Any and all data coming in from Veterans Health Information Systems and Technology Architecture (VistA) imaging

• Service record

• Secondary data sources from other research studies
• Finger or voice print
• Photographic image - Photographic images are not limited to images of the face.
• Vehicle identifiers and serial numbers, including license plate numbers
• Device identifiers and serial numbers
• Web URL
• Internet Protocol (IP) Address
• Any other characteristic that could uniquely identify the individual

PII Mapping of Components (Servers/Database)

RASP Azure consists of <**2**> key components (Research Data Repository/Analytic Study Marts). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by RASP Azure and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Researcher- and analyst-directed file shares and tables	Yes	Yes	Lab results, orders of medication, Records of outpatient visits, Surgery records, Patient personal information, Actionable genetic profile, international codes used to identify disease, etc. Veteran medical information, health records, scans, and more include: categories of tabular Electronic Health Records (her), and genomic data include: Phenomics from Central Data Warehouse (CDW) and similar sources; domains include: • PatientLabChem for test results Computerized Patient Record System (CPRS) Order for various procedures • Bar Code Medication Administration (BCMA) DispensedDrug for drugs prescribed • RxOutput for outpatient visits • Surgery for various procedures • Patient for identifying the person receiving treatment • Actionable Mutations for genomic basis of treatments • International Classification of Disease (ICD) 9/10 code table	Necessary to conduct research analysis and projects	RASP Azure provides all security safeguards as system owners. See infrastructure safeguards documented

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
			for codifying conditions and treatments • Oncology Raw for data files returned from analysis of patient's genome • Output for outpatient visits • Observational Medical Outcomes Partnership (OMOP) for a global standard vocabulary of medial terms and conditions • Genomics: FASTQ, Variant Call Format (VCF) formatted files • All data coming from commercial Picture Archiving and Communication System (PACS) and other medical devices including but not limited to Digital Imaging and Communications in Medicine (DICOM) files • Any and all data coming in from Veterans Health Information Systems and Technology Architecture (VistA) imaging • Service record • Secondary data sources from other research studies May include all 18 fields identified by Health Insurance Portability and Accountability Act (HIPAA) regulation such as: names, addresses, Social Security Numbers (SSN), dates of visits, etc. which are protected personal information: • Name • Address (all geographic subdivisions smaller than state, including street address, city county, and zip code) • All elements of dates related to an individual (including		

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
			birthdate, admission date, discharge date, date of death, and exact age if over 89) • Telephone numbers • Fax number • Email address • Social Security Number • Medical record number • Health plan beneficiary number • Account number • Certificate or license number • Vehicle identifiers and serial numbers, including license plate numbers • Device identifiers and serial numbers • Web Uniform Resource Locator (URL) • Internet Protocol (IP) Address • Finger or voice print • Photographic image - Photographic images are not limited to images of the face. • Any other characteristic that could uniquely identify the individual		
Data Governance for individual research projects will be managed by individual research teams	Yes	Yes	Same as listed above	Necessary to conduct research analysis and projects	We provide all of the security safeguards as system owners. See infrastructure safeguards documented

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Data sources are researcher- and analyst-directed file shares and tables.

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

Not Applicable

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

Not Applicable

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Information is extracted as electronic transmission from other systems, e.g., researcher- and analyst-directed file shares and tables. Information is extracted using a database client, stored on a server and then transferred to the VA RASP repository. All research files are handled electronically after passing the security approval processes of DART and IRB.

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

Not applicable.

1.4 How will the information be checked for accuracy? How often will it be checked?
These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Information is checked at the 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 researcher- and analyst-directed file shares and tables 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 RASP Azure to ensure that it falls within acceptable ranges and outliers are removed from the data set.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

Not Applicable

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:

OBJ(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. Version Date: February 27, 2020 Page 10 of 19.

As stated in Privacy Act Systems of Record Notice (SORN) 34VA10, "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 <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. (*Work with your System ISSO to complete this section)*

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: There is a risk that data contained in the RASP Azure 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. RASP Azure 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 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.

All data fields listed below will be used to support VA-sanctioned research to improve veteran's health by authorized researchers. RASP Azure's infrastructure platform connects to data source to run large research studies.

- **Name**: Name is used to identify Veterans and match data across different data sources
- **Social Security Number:** Last four is used as secondary identifier to match data
- **Date of Birth**: Date of birth is used for analytics projects as age is often related to health outcomes

- **Personal Mailing Address:** Current address is important for noting context of location, as location systematically affects health outcomes
- **Personal Phone Number(s):** Phone number is an additional identifier that is part of the researcher- and analyst-directed file shares and tables
- **Personal Fax Number:** Fax number is an additional identifier that is part of the researcher- and analyst-directed file shares and tables
- **Personal Email Address:** Email is an additional identifier that is part of the researcher- and analyst-directed file shares and tables
- **Emergency Contact Information** (Name, Phone Number, etc. of a different individual)
- **Health Insurance Beneficiary Numbers Account numbers:** Used as secondary identifier to match data
- **Certificate/License numbers:** Additional identifier that is part of the researcher- and analyst-directed file shares and tables
- **Vehicle License Plate Number:** Used as secondary identifier to match data
- **Internet Protocol (IP) Address Numbers:** Unique address to identify hardware devices
- **Medications:** Medications are used in analytics projects as important data elements to understand health outcomes
- **Medical Records:** Previous medical records are used in analytics projects to understand the longitudinal course of health and health concerns among service members
- **Race/Ethnicity:** Race is used for analytics projects as race and ethnicity systematically affect health
- **Medical Record Number:** Medical Record Number is an additional identifier that is part of the researcher- and analyst-directed file shares and tables
- **Gender:** Gender is used for analytics projects as gender systematically affects health outcomes
- **Military History/Service Connection:** Military History/Service Connection is an important data element for analytics projects to understand the historical context behind current health and wellness

Other Data Elements

- **PII and PHI as held in researcher- and analyst-directed file shares and tables:** Name is used to identify Veterans and match data across different data sources
- **PatientLabChem for test results:** Input for modeling and prediction
- **CPRS Order for various procedures:** Input for modeling and prediction
- **BCMA DispensedDrug for drugs prescribed:** Input for modeling and prediction
- **RxOutpat for outpatient visits:** Input for modeling and prediction
- **Surgery for various procedures:** Input for modeling and prediction
- **PatientID for identifying the person:** PatientID is an additional identifier that is part of the researcher- and analyst-directed file shares and tables
- **Actionable Mutations for genomic basis of treatments:** Input for modeling and prediction
- **ICD9/10 code table for codifying conditions and treatments:** Input for modeling and prediction
- **Oncology Raw for data files returned from analysis of patient's genome:** Input for modeling and prediction
- **Output for outpatient visits:** Input for modeling and prediction

- **OMOP for a global standard vocabulary of medial terms and conditions:** Input for modeling and prediction
- **Genomics: FASTQ, Variant Call Format (VCF) formatted files:** Input for modeling and prediction
- **All data coming from commercial PACS and other medical devices including but not limited to DICOM files:** Input for modeling and prediction
- **Any and all data coming in from VistA imaging:** Input for modeling and prediction
- **Service record:** Input for modeling and prediction
- **Secondary data sources from other research studies:** Input for modeling and prediction
- **Finger or voice print:** Input for modeling and prediction
- **Photographic image - *Photographic images are not limited to images of the face***: images are important objective data elements for analytics projects to understand health outcomes
- **Device identifiers and serial numbers**: Device identifiers and serial numbers may be additional identifiers that are part of the researcher- and analyst-directed file shares and tables
- **Web URL**: Web URL is an additional identifier that may be part of the researcher- and analyst-directed file shares and tables
- Any other characteristic that could uniquely identify the individual

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

Data sets are collected and tools such as (planned) Azure Machine Learning (ML) are planned to be used in performing complex analytical tasks to perform work studies.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

Not Applicable

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

SC-28.1; RASP Azure Platform protects the confidentiality and integrity of information storage in S3. All RASP Azure Blob Storage enforces bucket encryption. If a Blob Storage Container is created that isn't encrypted, Turbot (governance tool) will automatically encrypt the bucket. SC-28.2; RASP Azure defines information at rest as any data that is stored in Azure Blob Storage Containers that will automatically be encrypted.

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

Cryptographic measure enforcing encryption such as TLS 1.3/AES-256 and hashing algorithm which is FIPS 140-2 Compliance, are in place to maintain Confidentiality and Integrity of PII/PHI data within this RASP system.

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

To protect veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:

1. The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified. 2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability. 3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers. 4. Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. ***Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e., denial of access) that are in place if an individual is inappropriately using the information.***

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

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

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

2.4a How is access to the PII determined?

Only VA accredited staff have access to instances in the VA Enterprise Cloud (VAEC) and data on a per protocol basis. List of approved personnel is maintained in Data Access Request Tracker (DART) system on prem. An Institutional Review Board (IRB) has oversight for each protocol. All research activity is pre-approved by local privacy officer and research Information System Security Officer (ISSO). This system uses Federal Information Security Management Act (FISMA) standard processes for approving and monitoring access. This system is continually monitored and audited for compliance to FISMA security standards

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

Yes, criteria procedures and controls are documented within respective DART and IRB processes. The RASP Azure Access Control Standard Operating Procedure (SOP) documents the criteria and responsibilities regarding access.

2.4c Does access require manager approval?

All research activity is pre-approved by local privacy officer and research ISSO

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

The RASP Azure system uses centralized logging system (CLS) to monitor and log information. This system is continually monitored and audited for compliance to FISMA security standards.

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

The RASP Information System Owner (ISO) is responsible for safeguarding the PII.

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*

- Name
- Social Security Number
- Date of Birth
- Current Medications
- PII and PHI as held in researcher- and analyst-directed file shares and tables
- PatientLabChem for test results
- CPRS Order for various procedures
- BCMA DispensedDrug for drugs prescribed
- RxOutpat for outpatient visits

- Surgery for various procedures
- PatientID 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
- Outcome of any research

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

Data is retained in compliance with records schedule approved by the National Archives and Records Administration (NARA) and published on 7/13/2015.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:
Records are scheduled in accordance with Record Control Schedule (RCS) 10–1, 8300.6, Temporary Disposition; Cutoff at the end of the fiscal year after completion of the research project. Destroy six (6) years after cutoff. May retain longer if required by other Federal regulations or the European General Data Protection regulations. (DAA–0015–2015–0004, item 0032).

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes, records retention and destruction comply with the NARA approved Records Control Schedule, RCS-10

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

RASP Azure is a research system falling under 34VA10 (Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA). Record retention will fall under Research Investigator Files (8300-6) (Records Control Schedule RCS 10-1). This system will span the entire lifecycle of the project with a cutoff at the end of the fiscal year after completion of the research project. Destroy 6 years after cutoff and may retain longer if required by other Federal regulations.

Research Investigator Files Disposition Authority Number DM-0015-2015-0004-0032

Research records maintained by the investigator that span the entire lifecycle of the project and the records required by regulations such as the investigator's regulatory file. Records include, but are not limited to:

- Research protocol and all amended versions of the protocol; grant application; review committee correspondence (e.g., institutional review board, institutional animal care and use committee, research & development committee) including documents approved by the review committees
- Correspondence with ORD, regulatory entities, sponsor and/or funding source, correspondence
- Case report forms and supporting data (including, but not limited to, signed and dated informed consent forms and HIPM authorization forms)
- Documentation on each subject including informed consent, interactions with subjects by telephone or in person, observations, interventions, and other data relevant to the research study
- Data collected during the research including photos, video recordings, and voice recording, all derivative data, and derivative databases
- List of all subjects entered in the study and the cross-walk connecting the subjects name with the code used for each subject, subject compensation records
- Reports of adverse events, complaints, and deviations from IRS-approved protocol
- Data analyses
- Codes and keys used to de-identify and re-identify subjects' PHI
- Reports (including, but not limited to, abstracts and other publications)
- Research study correspondence not involving ORD, office of research oversight (ORO), sponsor, or funding source
- Correspondence and written agreements with the funding source or sponsor, ORD and applicable oversight entities such as IRB, research and development (R&D) committee, va office of research and oversight (ORO), va office of human research protections (OHRP) and FDA
- Research study correspondence not involving ORD, office of research oversight (ORO), sponsor, or funding source
- Signed and dated forms submitted to regulatory agencies
- Investigator's brochure
- Records related to the investigational drugs such as drug accountability records

- Monitoring and audit reports such as data safety monitoring board reports and audits by oversight entities
- Documents related to budget and funding
- Other forms required by policy and regulation

  Note: If the investigator leaves VA, all research records are retained by the VA facility where the research was conducted. If the grant is ongoing and the investigator leaves one VA facility to go to another VA facility, the investigator must obtain approval for a copy of relevant materials to be provided to the new VA facility's research office. The investigator is not the grantee, nor does the investigator own the data.

Link to full Outline of Records Schedule Items document:
https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-veterans-affairs/rg-0015/daa-0015-2015-0004_sf115.pdf

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

When records are no longer needed, the records may not be destroyed until VA/RASP obtains an approved records disposition authority from the Archivist of the United States. Records will be destroyed according to NIST Special Publication 800-88. Version Date: February 27, 2020 Page 13 of 29.

During the interim, for the lifecycle of the data, VA security protocols are followed throughout the system. RASP 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 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.

Data will be eliminated/transferred in accordance with the individual/research project plan or sub-agency policy (e.g., loan guarantee) in alignment with the researcher/analyst internal department requirement. Elimination and transmission of data will vary project-to-project (e.g., grant requirements have varying dates on elimination). There is no physical media; all data is on Microsoft Azure Government Cloud.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what

controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

Privacy Risk: 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 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.

There is a risk that the information contained in RASP will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: 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 environment where information is held and processed is protected by both OI& and the VA Enterprise Cloud/RASP security mechanisms. Furthermore, the was granted an ATO 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.

In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only as long as necessary.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Researcher- and analyst-directed file shares and tables	Extracting information; a patient's condition under investigation is used for analysis and modeling	Lab results, orders of medication, Records of outpatient visits, Surgery records, Patient personal information, Actionable genetic profile, international codes used to identify disease, etc. Veteran medical information, health records, scans, and more include: categories of tabular EHR, and genomic data include: Phenomics from CDW and similar sources; domains include: • PatientLabChem for test results Computerized Patient Record System CPRS Order for various procedures • Bar Code Medication Administration (BCMA) DispensedDrug for drugs prescribed • RxOutput for outpatient visits • Surgery for various procedures • Patient for identifying the person receiving treatment • Actionable Mutations for genomic basis of treatments • International Classification of Disease ICD9/10 code table for codifying conditions and treatments • Oncology Raw for data files returned from analysis of patient's genome • Output for outpatient visits • Observational Medical Outcomes Partnership (OMOP) for a global standard vocabulary of medial terms and conditions • Genomics: FASTQ, Variant Call Format (VCF) formatted files • All data coming from commercial PACS and other medical devices including but not limited to DICOM files • Any and all data coming in from VistA imaging • Service record • Secondary data sources from other research studies	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 processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		May include all 18 fields identified by HIPAA regulation such as: names, addresses, SSN, dates of visits, etc. which are protected personal information: • Name • Address (all geographic subdivisions smaller than state, including street address, city county, and zip code) • All elements of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89) • Telephone numbers • Fax number • Email address • Social Security Number • Medical record number • Health plan beneficiary number • Account number • Certificate or license number • Vehicle identifiers and serial numbers, including license plate numbers • Device identifiers and serial numbers • Web URL • Internet Protocol (IP) Address • Finger or voice print • Photographic image - Photographic images are not limited to images of the face. • Any other characteristic that could uniquely identify the individual	
Temporary individual tenants built for individual research projects	Extracting information; a patient's condition under investigation is used for analysis and modeling	Same as above	VA internal secure network HTTPs and FIPS 140- 2

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

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

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

Follow the format below:

> **Privacy Risk:** 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 Version Date: February 27, 2020 Page 17 of 29 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, 24hour 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***
VA Academic Affiliates	Many VA research projects are conducted with an Academic Affiliate, per VA research guidance and policy	Lab results, orders of medication, Records of outpatient visits, Surgery records, Patient personal information, Actionable genetic profile, international codes used to identify disease, etc. Veteran medical information, health records, scans, and more include: categories of tabular Electronic Health Records (EHR), and genomic data include: Phenomics from Central Data Warehouse (CDW) and similar sources; domains include: • PatientLabChem for test results Computerized Patient Record System CPRS Order for various procedures • Bar Code Medication Administration (BCMA) DispensedDrug for drugs prescribed • RxOutput for outpatient visits • Surgery for various procedures • Patient for identifying the person receiving treatment • Actionable Mutations for genomic basis of treatments • International Classification of Disease ICD9/10 code table for codifying conditions and treatments • Oncology Raw for data files	Per the affiliate agreements found on the affiliate site: https://www.va.gov/oaa/affiliation-agreements.asp	Transmission method will be Azure Storage Service Encryption or Azure Disc Encryption to comply with FIPS 199

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*
		returned from analysis of patient's genome • Output for outpatient visits • Observational Medical Outcomes Partnership (OMOP) for a global standard vocabulary of medial terms and conditions • Genomics: FASTQ, Variant Call Format (VCF) formatted files • All data coming from commercial PACS and other medical devices including but not limited to DICOM files • Any and all data coming in from VistA imaging • Service record • Secondary data sources from other research studies May include all 18 fields identified by HIPAA regulation such as: names, addresses, SSN, dates of visits, etc. which are protected personal information: • Name • Address (all geographic subdivisions smaller than state, including street address, city county, and zip code) • All elements of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89) • Telephone numbers • Fax number • Email address • Social Security Number • Medical record number		

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*
		• Health plan beneficiary number • Account number • Certificate or license number • Vehicle identifiers and serial numbers, including license plate numbers • Device identifiers and serial numbers • Web URL • Internet Protocol (IP) Address • Finger or voice print • Photographic image - Photographic images are not limited to images of the face. • Any other characteristic that could uniquely identify the individual • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Medications • Medical Records • Race/Ethnicity • Gender • Military History/Service Connection		
National Institutes of Health (NIH)	Results of studies or other grant deliverables uploaded on grantor's system	Same as listed above	NIH https://sharing.nih.gov/data-management-and-sharing-policy/about-data-management-and-sharing-policies/data-management-and-	Uploads to the NIH site

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***
			sharing-policy-overview	

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: The risks are documented in the affiliate agreements outside the OIT. Sharing with NIH is common practice for VA researchers as part fulfilling their grant obligations. NIH maintains systems for upload, as they are system owners.

Mitigation: Ensure before doing any connection with affiliates, that there is an affiliate agreement in place. For NIH, only use federally approved system sharing and platforms.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

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.
SORN Number: 34VA10 SORN Name: 34VA10 Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA

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

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

Not applicable see *6.1a* above

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

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 waiver and/or authorization.

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

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

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

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

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

Follow the format below:

Privacy Risk: Sufficient notice is always provided, if there is no consent then there is no data collection. Consent is continually re-evaluated in every new protocol review and is approved by the associated VA IRB team, privacy officer (PO) and information systems security officer (ISSO).

There is a risk that an individual may not understand why their information is being collected or maintained about them.

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

This risk is of an individual not understanding why their information is being collected is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries when there is a change in regulation. Employees and contractors are required to review, sign, and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

VHA 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

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

Not applicable

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

Privacy Act System of Record Notice (SORN) 34VA10 Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA. The procedure outlined in the SORN complies with VHA Directive 1605.01, Paragraph 7 and VA Regulation 38 CFR § 1.577.

https://www.govinfo.gov/content/pkg/FR-2021-06-23/pdf/2021-13141.pdf

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 are made aware of procedures for correcting their information in multiple ways. First, this information in published in the Privacy Act SORN 34VA10 Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA. The procedure

outlined in the SORN complies with VHA Directive 1605.01, Paragraph 7 and VA Regulation 38 CFR § 1.577.

https://www.govinfo.gov/content/pkg/FR-2021-06-23/pdf/2021-13141.pdf

In addition, all Veterans are provided a VHA Notice of Privacy Practices every three years, upon request or when significant changes are made. The VHA NOPP provides information on how to request and amend to their PHI maintained by VHA. Lastly, this information is contained in VHA Directive 1605.01, Privacy and Release of Information, which is available to the public online at http://www.va.gov/vhapublications/publications.cfm?pub=2&order=asc&orderby=pub_ Individuals wishing to obtain more information about access may write or call the Director of Operations, Research and Development (12), Department of Veterans Affairs, 810 Vermont Ave., NW. Washington, DC

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Not applicable, formal redress is provided as stated above in section 7.3.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

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

Follow the format below:

Privacy Risk: The individual may also seek to access (or redress) records about them held within RASP Azure and become frustrated with the results of their attempt.

Mitigation: Active participants in VA research studies have the ability to redress and correct information directly with the study's research staff. Through informed consent and HIPAA authorization forms the active participants are informed of what information is being collected for the study and what purpose the information will be used for.

Strict policy defined in VHA 1200.05; Requirements for the Protection of Human Subjects in Research mitigates the risk that information collected for a study will be used for other purposes.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

The RASP Azure organization grants access by developing roles to separate duties within the organization. The Admin. role (tied to 0account) grants users full access to the application and the Researcher role (tied to PIV) allows users to create and access their studies. Furthermore, within Azure, the rasp-admin role grants users full access to services allowed via Azure Managed Applications, while the Project-admin role grants users access to most services, except IAM; both of these roles must be requested via ePAS and require a 0account. For read-only access, users must submit a WFM ticket.

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

The ORD Administrator role is responsible for establishing PII criteria and Data copy into RASP Azure from research data sources.

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Administrator roles: Admin roles (tied to 0account) that grants users full access to the application Azure: rasp-admin role that grants users full access to services allowed via Azure Managed Applications and Project-admin role grants users access to most services, except IAM.

User roles: Researcher roles (tied to PIV) that allows users to create and access their studies. Azure: Read-only roles (tied to PIV) for viewing reports.

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.

Yes. 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 Version Date: February 27, 2020 Page 25 of 29 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?

8.4a If Yes, provide:

1. *The Security Plan Status: In Process*
2. *The System Security Plan Status Date: In Process*
3. *The Authorization Status: In Process*
4. *The Authorization Date: N/A*
5. *The Authorization Termination Date: N/A*
6. *The Risk Review Completion Date: N/A*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH): HIGH*
8.

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

8.4b If No or In Process, provide your Initial Operating Capability (IOC) date.

TBD

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

The RASP Azure system operates within the VAEC GovCloud with a FedRAMP authorization in process. Cloud models include PaaS, COTS, and IaaS service.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

N/A

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

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

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

N/A

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

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

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

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	Authority and Purpose
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	Accountability, Audit, and Risk Management
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	Data Quality and Integrity
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	Data Minimization and Retention

ID	Privacy Controls
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	Individual Participation and Redress
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	Security
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	Transparency
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	Use Limitation
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Digitally signed by Kimberly E. Murphy 183320
Date: 2023.06.21 15:23:30 -04'00'

Privacy Officer, Kimberly Murphy

Albertino M. Estacio 119921

Digitally signed by Albertino M. Estacio 119921
Date: 2023.06.21 13:41:37 -07'00'

Information System Security Officer, Albert Estacio

Christopher L. Cardella 208768

Digitally signed by Christopher L. Cardella 208768
Date: 2023.06.22 09:44:09 -05'00'

Information System Owner, Christopher Cardella

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).

SORN Number: 34VA10 SORN Name: 34VA10 Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA

https://www.govinfo.gov/content/pkg/FR-2021-06-23/pdf/2021-13141.pdf

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices