Privacy Impact Assessment for the VA IT System called:

Robotic Process Automation (RPA)

Veterans Affairs Central Office (VACO)

Enterprise Program Management Office (EPMO)

eMASS ID# 1399

Date PIA submitted for review:

02/21/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	OITPrivacy@va.gov and Tonya.Facemire@va.gov	202-632-8423
Information System Security Officer (ISSO)	Robert Hall	Robert.Hall7@va.gov	216-522-3530 x3710
Information System Owner	Paul Haberl	Paul.Haberl1@va.gov	254-981-8337

Abstract

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

The Robotic Process Automation (RPA) platform is used to automate processes so that personnel can focus on high-value vs. low-value processes. This project provides a low-code/no-code platform that includes artificial intelligence to provide automation for business customer needs. The RPA platform provides business owners the ability to take their rote/repetitive business processes and automate them using software scripts (bots). The bot development can be done either using OIT resources or business users (citizen developers) due to the platform's low-code/no-code capabilities.

The RPA platform, consisting of Blue Prism, UIPath Automation Suite, and UIPath Orchestrator, are hosted in the Veteran Affairs Enterprise Cloud Microsoft Azure Government (MAG) platform. Connection via Hypertext Transfer Protocol Secure (HTTPS) port 443 for the data in transit is made to allow the bot to run. There are use cases where sensitive data (PII and PHI) may be transmitted through the platform, and temporarily stored. Most work is contained within the source system. Bots run as a standard user within the source systems. All collected PII/PHI is covered by source system's PTAs/PIAs.

Overview

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

1 General Description

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

Robotic Process Automation is owned by the Enterprise Management Program Office.

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

The purpose of the platform is to provide automation and machine learning for dashboards, data connectors and application connectors. Some bots will be attended bots and those require users to trigger them. Unattended bots run on their timed schedule. Bots follow the same rules as human users. They are subject to same rules/authorizations. Bots can be customized to meet the needs of the organization as it continuously runs in the background and can mimic certain human actions such as moving files, copying data and logging into application.

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

VA Controlled / non-VA Owned and Operated IS.

2. Information Collection and Sharing

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

RPA provides support VA-wide and supports approximately 2,000+ users.

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

While the RPA system does not act as a data retention/storage platform, in some cases data will be temporarily cached to facilitate the automated script operation. For most automation processes, the scripts process records within seconds or minutes. However, a bot could perform work that requires many hours of processing. To ensure the data cached to facilitate such processes is limited to minimize risk, RPA COE project management has implemented the design standard that temporary caching of data will be limited to the minimum amount of data for the minimum amount of time necessary to facilitate the "as designed" operation of the bot. In all cases, the automation design, development, and testing processes will enforce this standard and clean-up processes will be incorporated within automation workflows to ensure target system data is not stored in violation of this design standard. Data elements are not collected by RPA but can be processed or retained on the platform. Name, SSN, DOB, Mother's Maiden Name, Mailing Address, Zip Code, Phone Number(s), Fax Number(s), Email address, Emergency Contact Information (Name, Phone Number, etc. of a different individual), Financial Account Information, Health Insurance Beneficiary numbers/Account numbers, Current Medications, Previous Medical Records, Race/ethnicity

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

RPA transmits data, it does not store data in a repository to disclose or share data, with Microsoft Active Directory.

The system will be used throughout VA after undergoing the RPA Intake Process. We will regularly track and update the PTA/PIA to include sites and use cases:

- ***Information Technology Budget and Finance (ITBF):***
    - *BTT FCR Approvals: process approvals of Financial Change Requests (FCR) that takes place within the Budget Tracking Tool (BTT) environment and through email/Outlook and Excel. (No PII/PHI)*
    - *BTT Misalignment Analysis: checks for misalignment of Portfolio, Investment, Congressional Program, and Congressional Project information in BTT against the assigned Budget Structure, modifies records as needed, and notifies ITBF stakeholders via email. (No PII/PHI)*
    - *Status of Allowance: logs into VHA Support Service Center (VSSC), creates a daily Status of Allowances report with Financial Management System (FMS) running balances for IT Funds and COVID IT Funds, and saves the report to ITBF shared location. The reports are then processed in Excel using existing business rules and compared to Integrated Funds Distribution, Control Point Activity, Accounting and Procurement System (IFCAP) data to identify discrepancies, and an email is generated to the correct POC with results. OUTLOOK (No PII/PHI)*
    - *BF Validate BTT Data: the Budget Formulation (BF) Validate Data process takes place using Budget Tracking Tool (BTT) and Microsoft Excel. The process involves identification of misaligned or erroneous budget records (validating against Budget*

Structure, TBM Structure, and other Business Rules), and aligning or correcting those records as needed. Data touched by this automation includes financial data. (No PHI or PII)

- ***FedRAMP SSP Conversion—****to automate the process of creating two Excel documents needed for the RMF Step 2. The process involves cutting and pasting correct data from Cloud Service Provider's (CSP) System Security Plans (SSP) (Word) into two separate Excel documents – one for the -E (Enterprise) package and one for the -F (FedRAMP) package. These Excel documents are delivered to a shared folder by the bot for manual review and usage. Data touched by the automation includes system name, vendor name, SSP date, SSP version, and security control information and status. (No PHI or PII)*

- ***VBA National Call Center:***
  - *VBMS eFolder Person Search: Copy the SSN from the target system, Cisco Finesse Interactive Voice Response (IVR), and paste into the target system, VBMS, search bar and then open the 'eFolder' to view the Veteran's profile.*
  - *21-0845 Lookup and Validation: Search the Veteran's record in the target system, VBMS, for a 21-0845 Authorization form. Validate the key fields on the form are filled out and the form is signed.*
  - *0820 Report Routing: Open and read the PDF document then uploads the document to either DOMA via log in or VBMS via API.*

G. Is the system 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?

RPA is used VA-wide, as RPA is a cloud platform. PII is captured during the intake process, and upon approval, users adhere to RPA's security boundaries. All new use cases are thoroughly reviewed and must fall within the prescribed FIPS 199 security category.

3. Legal Authority and SORN

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 301; 38 U.S.C. 501; 40 U.S.C. 11331; 44 U.S.C 3544; Executive Order 9397; Homeland Security Presidential Directive 12; Federal Information Processing Standard 201–1.

146VA0005Q3/73 FR 16093 Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008) Point of Contact: Christopher Layton
The information in this system is provided by VA employees, contractors and anyone needing long term access to VA facilities and includes identifying information such as Social Security Number, Personal Identity Verification Card (PIV) information and the results of background investigations.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Section 501 and Section 7304.

192VA30/87 FR 36207 Veterans Affairs Profile-VA (10/23/2023)
The purpose of VA Profile is to source authoritative common and shared information about VA customers, starting with contact information. Information in this system of records is mastered, meets VA data quality standards, and allows VA customers to use a

single touchpoint to update contact information and other key data. VA Profile will enable synchronization of information to provide each VA administration with an updated, accurate, and timely customer Profile. VA Profile is the authoritative storage repository for certain common customer data, specifically contact information, and VA Profile functions as a pass through with synchronization of customer Profile data stored in other VA authoritative data sources.

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?*

The SORN does not require amendment or revision and approval. RPA will be hosted on VAEC's Microsoft Azure Government platform.

4. System Changes

J. *Will the completion of this PIA will result in circumstances that require changes to business processes?*
The completion of this PIA will not result in circumstances that require changes to RPA's business processes.

K. *Will the completion of this PIA could potentially result in technology changes?*

Completion of this PIA will not result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☒ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☒ Personal Fax Number
☒ Personal Email Address
☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☒ Financial Information
☒ Health Insurance Beneficiary Numbers Account numbers
☒ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☒ Medical Record Number
☒ Gender
☒ Integrated Control Number (ICN)
☐ Military History/Service Connection
☒ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements: Internal Control Number, and Station ID

PII Mapping of Components (Servers/Database)

Robotic Process Automation consists of 2 key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Robotic Process Automation 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 server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Blue Prism Enterprise	Yes	Yes	VA Name, Email Address	Data Elements are not collected by RPA but can be	RPA uses Federal Information Processing

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

				processed or retained on the platform.	Standards (FIPS) compliant Advanced Encryption Standard (AES)-256 algorithm for data encryption at rest and Hypertext Transfer Protocol Secure (HTTPS) port 443 for the data in transit
UIPath Orchestrator, and UIPath Automation Suite	Yes	Yes	VA Name and Email Address, IP Addresses, Name, SSN, DOB, Mother's Maiden Name, Mailing Address, Zip Code, Phone Number(s), Fax Number(s), Email address, Emergency Contact Information (Name, Phone number, etc. of a different individual), Financial Account Information, Health Insurance Beneficiary numbers/Account numbers, Current Medications, Previous Medical Records, Race/ethnicity	Data Elements are not collected by RPA but can be processed or retained on the platform.	RPA uses Federal Information Processing Standards (FIPS) compliant Advanced Encryption Standard (AES)-256 algorithm for data encryption at rest and Hypertext Transfer Protocol Secure (HTTPS) port 443 for the data in transit

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?

VistA, for Open Encounters

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.

RPA is not an authoritative source for any data. Data is pulled from various VA systems to support automation of business processes.

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

RPA does not provide aggregated data.

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?

Data Elements are not collected by RPA but can be transmitted or temporarily retained on the platform.

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

RPA does not utilize forms to collect data.

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.

RPA will not be checking the information for accuracy. Robotic Process Automation platform is only transmitting the information and does not collect information directly from an individual.

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

RPA does not check for accuracy.

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

RPA uses the following SORNs for the transmitting of information:

> AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 301; 38 U.S.C. 501; 40 U.S.C. 11331; 44 U.S.C 3544; Executive Order 9397; Homeland Security Presidential Directive 12; Federal Information Processing Standard 201–1.
> 146VA0005Q3/73 FR 16093 Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008)
> The information in this system is provided by VA employees, contractors and anyone needing long term access to VA facilities and includes identifying information such as Social Security Number, Personal Identity Verification Card (PIV) information and the results of background investigations.
>
> AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Section 501 and Section 7304.
> 192VA30/87 FR 36207 Veterans Affairs Profile-VA (10/23/2023)
> The purpose of VA Profile is to source authoritative common and shared information about VA customers, starting with contact information. Information in this system of records is mastered, meets VA data quality standards, and allows VA customers to use a single touchpoint to update contact information and other key data. VA Profile will enable synchronization of information to provide each VA administration with an updated, accurate, and timely customer Profile. VA Profile is the authoritative storage repository for certain common customer data, specifically contact information, and VA Profile functions as a pass through with synchronization of customer Profile data stored in other VA authoritative data sources.
> Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, SORN 79VA10 / 85 FR 84114 (Link)

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Robotic Process Automation does not collect information directly from the individual, there is still risk of Personally Identifiable Information (PII), Personal Health Information (PHI), and other data that may identify an individual being breached or accidentally disclosed to inappropriate parties or the public. It could result in personal and financial harm to the individuals impacted, and adverse negative effects to the VA.

Mitigation: Data temporarily stored, and transmitted by RPA will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. Data stored at rest will be encrypted using 256-bit Advanced Encryption Standard (AES-256) and Hypertext Transfer Protocol Secure (HTTPS) port 443 for the data in transit. All systems and individuals with access to RPA will be approved, authorized, and authenticated before access is granted by VA Project Manager and System Owner. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system that will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

Robotic Process Automation platform is only transmitting the information and does not collect information directly from an individual. All data elements are only transmitted by automations/bots on the platform.

PII/PHI Data Element	Internal Use	External Use
Name	Identification purposes	Not used
SSN	Identification purposes	Not used
DOB	Identification purposes	Not used
Mother's Maiden Name	Identification purposes	Not used
Mailing Address	Identification purposes	Not used
Zip Code	Identification purposes	Not used
Phone Number(s)	Identification purposes	Not used
Fax Number(s)	Identification purposes	Not used
Email Address	Identification purposes	Not used
Emergency Contact Information	Identification purposes	Not used
Financial Account Information	Identification purposes	Not used
Health Insurance Beneficiary Numbers/Account Numbers	Identification purposes	Not used
Current Medications	Claims/Eligibility	Not used
Previous Medical Records	Claims/Eligibility	Not used
Race/Ethnicity	Claims/Eligibility	Not used
Internal Control Number and Station ID/VA Site/Clinic	Identification purposes	Not used
IP Addresses	User location	Not used
Visit Date/Time	Communication with patient	Not used
Visit Type	Communication with patient	Not used
Days Elapsed	Communication with patient	Not used
Visit Type	Communication with patient	Not used
Required Actions	Communication with patient	Not used
Provider and Provider Email	Identification purposes	Not used

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

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

RPA transmits the information and does not analyze the information going through the platform. RPA transmit information internally with approved VA systems.

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.

RPA does not create or make available new or previously unutilized information about an individual.

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?

RPA uses Federal Information Processing Standards (FIPS) compliant Advanced Encryption Standard (AES)-256 algorithm for data encryption at rest and Hypertext Transfer Protocol Secure (HTTPS) port 443 for the data in transit. MAG also has the following in place: Encryption of data at rest and data in transit (SSL, TLS). FIPS 140-2 compliant. Automated tools are used to validate and enforce data at rest controls continuously. Encryption keys and certificates are stored securely and rotated at appropriate times with strict access control.

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

RPA uses Federal Information Processing Standards (FIPS) compliant Advanced Encryption Standard (AES)-256 algorithm for data encryption at rest and Hypertext Transfer Protocol Secure (HTTPS) port 443 for the data in transit.

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

RPA uses Federal Information Processing Standards (FIPS) compliant Advanced Encryption Standard (AES)-256 algorithm for data encryption at rest and Hypertext Transfer Protocol Secure (HTTPS) port 443 for the data in transit.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

<u>Principle of Transparency:</u> 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?

There is no access to PII through RPA. Robotic Process Automation platform is only transmitting the information and does not collect information directly from an individual. Please refer to the source system's PIA for how the PII/PHI is collected. Bots must log all Bot activity. Attended Bots' logs must be reviewed weekly by the RPC and include the capability for a complete audit trail of activities for use by VA auditors, including data needed to identify abnormal spikes in activity, access of specific systems, and use of privileged accounts. For Unattended Bots, Orchestrator must be configured to provide for verbose logging of all robot activities. The platform also has controls in place to ensure the data being processed is protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all VA employees, and VA contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA has implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems.

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

Yes, information regarding access can be found in RPA's AC SOP, which is reviewed on an annual basis, or when changes occur in the procedures or regulations.

2.4c Does access require manager approval?

Yes, access to RPA requires ISO's or ISO designee.

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

RPA's technical team are the only ones with access to the platform, but they do not have clear text access to the PII—any temporarily retained PII is encrypted.

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

The Enterprise provisions privileged user accounts based on request submitted by the system which requires approval from ISO or designee. Access to perform administrative functions and with access to security relevant information (not including PII as RPA admin have no access to the PII that is temporarily stored on the platform) are based on role and security group membership and require NMEA account and token.

Section 3. Retention of Information

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

3.1 What information is retained?

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

Data Elements are not collected by RPA but can be processed or retained on the platform.

- Name
- SSN
- DOB
- Mother's Maiden Name
- Mailing Address
- Zip Code
- Phone Number(s)
- Fax Number(s)
- Email address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Financial Account Information
- Health Insurance Beneficiary numbers/Account numbers
- Current Medications
- Previous Medical Records
- Race/ethnicity

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.*

While the RPA system does not act as a data retention/storage platform, in some cases data will be temporarily cached to facilitate the automated script operation. For most automation processes, the scripts process records within seconds or minutes. However, a bot could perform work that requires many hours of processing. To ensure the data cached to facilitate such processes is limited to minimize risk, RPA COE project management has implemented the design standard that temporary caching of data will be limited to the minimum amount of data for the minimum amount of time necessary to facilitate the "as designed" operation of the bot. In all cases, the automation design, development, and testing processes will enforce this standard and clean-up processes will be incorporated within automation workflows to ensure target system data is not stored in violation of this design stand.

Primary storage is the queue/database, as bots pull data and store in the queue, which could potentially be used for the next bot/automation. PII/PHI remains encrypted in this process. The queue/database follows OI&T's general record retention schedule: Data in queue remains for 14 days and is then automatically purged. Information stored in RPA lives in databases hosted in VAEC Azure. Physical media sanitation requirements are inherited from VAEC Azure. RPA COE project management has implemented the design standard that temporary caching of data will be limited to the minimum amount of data for the minimum amount of time necessary to facilitate the "as

designed" operation of the bot. In all cases, the automation design, development, and testing processes will enforce this standard and clean-up processes will be incorporated within automation workflows to ensure target system data is not stored in violation of this design standard.
Admin Users (Name, Organization, Email Address): Inactive Accounts are identified and pruned after 90 days.
Cached Data: Cached and queued data remains for 14 days and is then automatically purged.

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?

RPA uses the OI&T Record Control Center 005-1 Page 46, PART I. SUBJECT/FUNCTIONAL RECORDSSECTION M. ELECTRONIC RECORDS Item No 1, b. Electronic files or records used to create or update a master file, including, but not limited to, work files, valid transaction files, and intermediate input/output records. Disposition: Delete after information has been transferred to the master file and verified.

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

OIT RCS 005-1 Page 46, PART I. SUBJECT/FUNCTIONAL RECORDSSECTION M. ELECTRONIC RECORDS Item No 1, b. electronic files or records used to create or update a master file, including, but not limited to, work files, valid transaction files, and intermediate input/output records. Disposition: Delete after information has been transferred to the master file and verified.

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.

This is primarily inherited from VAEC Azure, where RPA is hosted. Rules:

RPA is not a system of records. RPA transfers data from one VA system to another VA system. Those front and backend systems are the systems of record and are the official record repository.
Admin Users (Name, Organization, Email Address): Inactive Accounts are identified and pruned after 90 days.
Cached Data: Cached and queued data remains for 14 days and is then automatically purged.

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.

RPA does not use or process PII for testing/training/research.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (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: There is a risk that the information temporary retained by RPA could 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: To mitigate the risk posed by temporarily retained information, RPA adheres to the OIT RCS 005-1 Page 46, PART I. SUBJECT/FUNCTIONAL RECORDSSECTION M. ELECTRONIC RECORDS Item No 1, b. electronic files or records used to create or update a master file, including, but not limited to, work files, valid transaction files, and intermediate input/output records. Disposition: Delete after information has been transferred to the master file and verified. Queues are automatically set at 2 weeks.

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***
Active Directory	Identify User for Access	• VA Employee Name • Email Address	Lightweight Directory Access Protocol (LDAP)
VistA	Notification to provider of Open Encounters	• Clinic • Patient • Last 4 Social • Visit Date/Time • Days Elapsed • Visit Type • Provider	File Transfer Protocol (FTP)

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*
		• Provider Email • Required Actions • VA Site	

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: There is a risk that information may be shared with unauthorized VA personnel.

Mitigation: Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including annual employee security and privacy training, and required reporting of suspicious activity.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: There is no external sharing.

Mitigation: There is no 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 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.

RPA does not collect information directly from individuals. Systems that have bots doing so should have that tracked in their own system PTAs/PIAs.

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

RPA does not collect information, and thus, does not provide notice of collection.

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.

RPA does not collect information, and thus, does not provide notice of collection.

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.

No information is collected directly by RPA, so there is no opportunity to decline to provide information.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent

is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

Any right to consent to uses of the information would be handled by the source system and can be found in the source system's PIA.

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

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

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

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

Privacy Risk: There is a risk that an individual may not receive notice that their information is being transmitted by RPA.
Mitigation: Privacy Impact Assessment (PIA) is made available for review online by the source system.

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.***

This is not applicable for RPA. However, source systems collecting information would provide guidance to Veterans and other individuals as to how they may request copies of their records

containing personal data from the medical facility's Release of Information (ROI) office. Please refer to the source system's PIA for how individuals may gain access to their information.

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)?

RPA is not a system of record. However, source systems collecting information would provide guidance to Veterans and other individuals as to how they may request copies of their records containing personal data from the medical facility's Release of Information (ROI) office. Please refer to the source system's PIA for how individuals may gain access to their information.

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?

RPA is not a system of record. However, source systems collecting information would provide guidance to Veterans and other individuals as to how they may request copies of their records containing personal data from the medical facility's Release of Information (ROI) office. Please refer to the source system's PIA for how individuals may gain access to their information.

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.

Please refer to the source system's PIA for guidance as to how individuals may correct inaccurate or erroneous information.

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.

Please refer to the source system's PIA for procedures regarding the correction of information.

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.

Please refer to the source system's PIA for alternatives to formal redress. RPA derives its data from the source systems. Individuals/typical bot users would not gain access to RPA platform.

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: There is a risk that erroneous information is placed into RPA via the feed from other VA systems.

Mitigation: If there is erroneous or inaccurate information, it should be addressed in the source system—any validation performed would merely be the Veteran personally reviewing the existing information before they accept it. Individuals are allowed to provide updated information for their records by submitting new forms or correspondence and indicating to the VA that the new information supersedes the previous data through the source systems' protocol.

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?

Requestor will create an Information Technology Request Portal (ITRP) ticket to request access to the roles needed which will be reviewed and granted by an RPA administrator.

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?

There are no users from other agencies who have access to RPA. The System Administrator(s) will approve and provide user access.

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.

System Administrator: Full access to all data except for encrypted PII. For audit/debugging purposes, System Admins could decrypt the PII using a securely stored encryption key. Data is encrypted in transit and at rest so PII/PHI is not visible. Role is granted through ISO approval only.
Operator/User: No access to PII
Developer: No access to PII
Digital Worker/Non-Person Entity (NPE): Has access to encryption key to access PII/PHI as required by the approved automation workflow. Potential access to temporary PII generated by user/digital worker.
Permissions to PII are granted from source systems to the user(s) for attended bots.

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.

RPA's VA contractors will have access to RPA, but because there is no PII/PHI being stored on the platform, they will not have access to the PII. All PII/PHI in encrypted at rest and in transit. Privacy and Security training is a requirement at VA, and all relevant VA-wide trainings are completed by all personnel annually. Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the HIPAA, VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the VA Privacy and Information Security Awareness training, which all personnel must complete via the VA's Talent Management System (TMS).

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.

Privacy and Security training is a requirement at VA, and all relevant VA-wide trainings are completed by all personnel annually. Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the HIPAA, VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the VA Privacy and Information Security Awareness training, which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. VA users with access to protected health information must complete mandatory HIPAA Privacy training annually in TMS.

Role based training:
3867205 Training for Elevated Privileges for System Access
1357076 Information Security Role-Based Training for System Administrators

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

Yes.

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 06/13/2023
3. *The Authorization Status:* 2 Year ATO
4. *The Authorization Date:* 08/22/2023
5. *The Authorization Termination Date:* 09/21/2025
6. *The Risk Review Completion Date:* 08/01/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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.***

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)*

RPA utilizes VA Enterprise Cloud Microsoft Azure Government (MAG) High Assessing and Platform as a Service (PaaS).

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*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.*

<<ADD ANSWER HERE>>

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.

<<ADD ANSWER HERE>>

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.

<<ADD ANSWER HERE>>

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).

<<ADD ANSWER HERE>>

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

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

Signature of Responsible Officials

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

TONYA FACEMIRE

Digitally signed by TONYA FACEMIRE
Date: 2024.03.07 13:33:03 -05'00'

Privacy Officer, Tonya Facemire

ROBERT HALL

Digitally signed by ROBERT HALL
Date: 2024.03.29 13:02:57 -04'00'

Information Systems Security Officer, Robert Hall

PAUL HABERL

Digitally signed by PAUL HABERL
Date: 2024.03.28 15:56:54 -05'00'

Information Systems Owner, Paul Haberl

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

HELPFUL LINKS:

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

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

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

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices

Office of Information & Technology (OI&T)
Records Control Schedule (RCS) 005-1