Privacy Impact Assessment for the VA IT System called:

Patient Recruitment and Enrollment System for MVP (RNE) Assessing

Veterans Health Administration

OI&T Enterprise Program Management Office (EPMO)

Date PIA submitted for review:

12-27-2022

System Contacts:

System Contacts

Title	Name	E-mail	Phone Number
Privacy Officer	Kimberly Murphy	Kimberly.Murphy@va.gov	781-331-3206
Information System Security Officer (ISSO)	Andre Davis	Andre.Davis2@va.gov	512-326-7422
Information System Owner	Christopher Brown	Christopher.Brown1@va.gov	202-270-1432

Abstract

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

The Million Veteran's Program (MVP) Patient Recruitment and Enrollment (RNE) System is an internal facing web-based application used as part of an electronic recruiting engine that allows VA representatives to register/enroll military veterans into the volunteer program for clinical genetic sampling under the MVP Program umbrella. This application gathers veteran's information and assigns a VA specific identifier to that veteran record.

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.

Patient Recruitment and Enrollment System for MVP (RNE) Assessing and OI&T Enterprise Program Management Office (EPMO)

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

The Million Veteran's Program (MVP) Patient Recruitment and Enrollment (RNE) System is an internal facing web-based application used as part of an electronic recruiting engine that allows VA representatives to register/enroll military veterans into the volunteer program for clinical genetic sampling under the MVP Program umbrella. This application gathers veteran's information and assigns a VA specific identifier to that veteran record.

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

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.

Number of individuals will exceed 1,000,000 and will reflect the volume of Veterans registered with the VA as the original recruitment pool. The typical client is Veterans registered with the VA for benefits.

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

RNE retrieves all contact information including various forms of SSNs from the CDW and stores them in our candidate database to use in identifying prospective participants so this would apply to our system. In addition self-reported surveys are stored in this system.

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

Participation involves the recruitment of participants, enrollments into the program, engagement for continued activity tracking and feedback to Veterans and staff. The Genomic Informatics System for Integrative Sciences (GenISIS) will identify veterans by searching the VA EMR data for veterans who have received VA medical care within the last three years. Patient contact information will be imported in to GenISIS and sent to an outside contracting mail center for MVP invitation mailings. the Patient Recruitment and Enrollment System (RNE) application provides interfaces and extension points to transact recruitment and enrollment data stores housed in the GenISIS (GIS) data store. In order to provide future extensibility, participants events in the data stores follow a parent-child design pattern.

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 system is operated centrally, primarily at AITC, and is accessed at over 70 additional VA locations through VA authentication systems (i.e., PIV cards) as well as approved contractors with ATOs. All access is controlled by the VA MVP Coordinating Centers as allowed under the existing ATOs and VA access policies.

3. Legal Authority and SORN

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

34VA10 Veteran, Patient, Employee, and Volunteer Research and Development Project Record- The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 531. The current ATO was granted 9/14/2022 and will expire 3/8/2023.

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?

No

D. System Changes

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

No

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

No

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

Self-reported data about health, gender, medications, medical conditions lifestyle, military exposures, mental health and substance use. Veteran appointments are stored.

PII Mapping of Components (Servers/Database)

The Patient Recruitment and Enrollment (RNE) application consists of multiple components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **The Patient Recruitment and Enrollment (RNE) application** 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
Candidatedb	Yes	Yes	Name, Last 4 of SSN, DoB, Address, Phone, Email	VA Research-Related Data	PGP, SSH, SFTP, HTTPS

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?

RNE collects information from VA data sources. For recruitment purposes, access to VistA, the national name and address file, the National Patient Care Database (NPCD), the Compensation and Pension Records Interchange (CAPRI), the Veterans Administration's Corporate Data Warehouse (CDW), and the Master Veteran Index (MVI) will be needed to link Veterans to their mailing addresses and telephone numbers. To ascertain the vital status of users identified in these data sources and eliminate decedents from the recruitment lists, the VA Beneficiary Information and Records Locator System (BIRLS) and the VA-Medicare data merged mortality data will be accessed for the most complete and up to date information. In addition, it collects contact event information from VA contacts with Veterans about the recruitment and enrollment processes and all research activities related to the research program. It also stores all self-reported research survey responses from Veterans.

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.

The Patient Recruitment and Enrollment System (RNE) application provides interfaces and extension points to transact recruitment and enrollment data stores housed in the GenISIS (GIS) data store. In order to provide future extensibility, participants events in the data stores follow a parent-child design pattern.

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

Genomic Informatics System for Integrative Sciences (GenISIS)

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?

The data is collected directly from the systems listed above and from the self-reported surveys that the Veterans send back to the VA contractor for scanning and transfer to the VA (under an ATO). Additionally, VA counselors for RNE and GENISIS enter contact event information into RNE based on interactions with Veterans.

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.

Please provide response here

OMB No. 2900-0884

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.

The VA counselor will directly enter the veteran's information into the RNE. The RNE has error checking where feasible to ensure the information is correct. RNE data is imported from VA healthcare databases. VA MVP staff can edit participant contact information in RNE that is provided by the participant as needed (name/phone/address changes, etc.). In these cases, VA MVP staff advise the participant to update the info with the VA – phone number is provided. MVP cannot provide these updates directly to VA – Veterans are given information on how to correct their contact information in VA systems.

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. If contact information is found to be incorrect the records will be updated to indicate a bad address.

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

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

The authority for the system is Veterans' Benefits: Functions of Veterans Health Administration, 38 U.S. Code § 7303, which states, in part:(a) (1) In order to carry out more effectively the primary function of the Administration and in order to contribute to the Nation's knowledge about disease and disability, the Secretary shall carry out a program of medical research in connection with the provision of medical care and treatment to veterans. Funds appropriated to carry out this section shall remain available until expended. Version Date: January 2, 2019Page 8 of 23(2) Such program of medical research shall include biomedical research, mental illness research, prosthetic and other rehabilitative research, and health-care-services research. A Health Insurance Portability and Accountability Act (HIPAA) authorization was obtained from individual patients under the MVP research study to access, collect and store their health information and blood sample(s) for future research use. As stated in Privacy Act Systems of Record Notice (SORN) 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. Additionally, the VA Central IRB has approved the protocol (10-02), consent and HIPAA authorization forms as well as a HIPAA waiver.

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: As with any IT system maintaining large robust data sets, there is a risk that data contained in RNE may be shared with unauthorized individuals or that authorized users may share it with other unauthorized users.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to complete the mission of the Office of Research and Development (ORD). Once an incident is reported, the VA makes all efforts to identify the parties involved in an incident, identify potential issues and concerns, and offer assistance to the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA is able to better protect the individual's information.
RNE will meet all VHA Security, Privacy, and Identity Management requirements including VA Handbook 6500 (see Appendix E and Appendix F). The RNE application shall be designed to comply with the applicable approved Enterprise Service Level Agreement (SLA).

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.

1) Name: Used to identify the veteran. 2) Social Security Number: Used to identify Veterans. 3) Date of Birth: Used to verify the identity of the veteran– Used for statistical reporting. 4) Mailing Address: Used to verify the identity of the veteran- communication. 5) Zip Code: Part of mailing address – Used for statistical reporting – communication. 6) Phone Number(s) – Communication with veteran. 7) Current Medications: Used to record current health and medical conditions of the veterans such as: Hepatitis C registry, Human Immunodeficiency Virus (HIV) registry, problems, diagnosis, therapeutic procedures, X-rays, laboratory tests, statistical reporting and operations. 8) Previous Medical History: Used to record the history of health and medical conditions of the veterans such as: Hepatitis C registry, Human Immunodeficiency Virus (HIV) registry, problems, diagnosis, therapeutic procedures, X-rays, laboratory tests, statistical reporting and operations. 9) Race/Ethnicity – used for statistical reporting and research. 10) VA Research-Related Data – use for data analysis as part of research study

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.

Research and statistical analysis tools relevant for MVP research for e.g. clinical datasets and phenotyping tools, ETL (Extract, Transfer and Load) database tools, etc..

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.

Patient Recruitment and Enrollment System (RNE) application only provides interfaces and extension points to transact recruitment and enrollment data stores housed in the GenISIS (GIS) data store. In order to provide future extensibility, participants events in the data stores follow a parent-child design pattern.

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?

All databases are encrypted. SSL connections are used for all connections. Only the application interfaces are used for input and display.

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

SSNs are stored in the database which is encrypted. SSL connections are used for all connections. Only the application interfaces are used for input and display. Only last 4 of SSNs can be displayed. When necessary to fully identify a veteran full social security numbers are typed in and displayed as typed. They cannot be retrieved and are not transferred.

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

Only research credentialled personnel have access. Participants do not have access.

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?

VA Training and Research Credentialing: VA staff accessing MVP RNE undergoes annual trainings in research ethics, HIPAA and security. These trainings are provided via the online Collaborative Institutional Training Initiative (CITI) program as well as the VA's Talent Management System (TMS). In order to access the system, staff must also undergo "MVP User Training" provided by MVP staff. They must also adhere to the MVP rules of conduct.

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

VA Records Management Policy (VA Handbook 6300.1) and the VA Rules of Behavior are in place to mitigate some of the risk that information is not handled properly. All VA annual privacy and security awareness training is recorded in the Talent Management System (TMS). The rules of behavior (VA handbook 6500 Appendix D) govern how veterans' information is used, stored, and protected.

2.4c Does access require manager approval?

VA IAM/MVI Authentication: All Veterans data in RNE is keyed to a valid VA GENISIS ID. Data entry by VA staff integrity is enforced by instantiation of a multi-factor authentication requirement for logging onto the system.

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

VA Network Authentication is used to restrict access to appropriate personnel. Access is monitored, tracked, and logged.

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

All research staff are responsible for protecting PII and the use of proper procedures pertaining to safe handling and prevention of inappropriate distribution of 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, Mailing Address, Zip Code, Phone Number(s), Current Medications, Previous Medical History, Race/Ethnicity and VA Research-Related Data.

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. 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 expected to be maintained for the duration of the MVP. VHA policy requires that all research records must be retained for a minimum of 5 years after the completion of a protocol and in accordance with VHA's Records Control Schedule (RCS 10-1), applicable FDA (Food and Drug Administration) and HHS (Health and Human Service) regulations, and then destroyed in accordance with VHA's RCS 10-1 requirements.

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

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

RNE 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.

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.

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA Handbook 6500.1, Electronic Media Sanitization. The Austin Information Technology Center (AITC) has an exception memorandum, dated 13 Apr 2015, allowing the center to locally destroy media. The memorandum lists specific methods of sanitization which are approved methods in accordance with VA 6500.1. Disposition of Printed Data: Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks and disposed of properly (when the approved records schedule permits destruction) by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers. AITC has a local shred contract (VA200R-1307) covering the destruction of printed data.

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.

For testing and training we use deidentified "Dummy Test Data".

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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 maintained by RNE 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 information retention, RNE adheres to the Records Schedule approved by NARA. When the retention date is reached for a record, the data is carefully disposed of by the approved method as described in Records Schedule in accordance with VA Handbook 6500.1 media and destruction policies.
Records Schedule Number DAA-0015-2015-0004 was approved by the National Archives and Records Administration (NARA) and published on 7/13/2015.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VHA Office for Analysis and Business Intelligence	Research requests for business analysis supporting veterans through VA statistical analysis, reporting and leadership decisions	• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number(s) • Current Medications • Previous Medical History • Race/Ethnicity	Secure electronic data transfer via online connection to VINCI database. File Transfer over Sockets Layer (SSL) /Transport Layer Security (TLS) Remote Desktop Communication (RDP over SSL/TLS)
VHA Office of Research Development and VA Researchers at VAMCs	Research request supporting VA research projects helping veterans by supporting information in medical and other research.	• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number(s) • Current Medications • Previous Medical History • Race/Ethnicity • VA Research-Related Data	Secure electronic data transfer via online connection to VINCI database. Remote Desktop Communication (RDP over SSL/TLS)

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 the risk of unauthorized access and impermissible disclosure which exists with any IT system maintaining IIHI/PHI to which individuals are given access. The data contained in RNE may be shared inadvertently with unauthorized individuals or authorized users may share it with other unauthorized individuals. Examples of this risk would be an unauthorized person breached the system or a VA sponsored user shares data outside of the VA boundary without legal authority.

Mitigation: Authorized users are required to sign the National Rules of Behavior (or Contractor Rules of Behavior) as part of the annual Privacy and Security Awareness training, which is documented in the VA Talent Management System (TMS).

RNE mitigates this privacy risk by requiring all users to have on file with their IRB of record a complete security and privacy awareness training, which includes appropriate and inappropriate uses and disclosures of the information accessible to them as part of their official duties. User activity in the system is monitored and audited. Should a user inappropriately use or disclose information, he or she is subject to loss of access and the disclosure will be referred to the appropriate internal investigation.

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 see attached MOU ISA, 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 Contractors	VA-approved Research Studies often need contractors to assist with data analysis	• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number(s) • Current Medications • Previous Medical History • Race/Ethnicity • VA Research-related data	34VA10 RU#19 HIPAA Privacy Rule (45 CFR 164.512(i)) MOU	As noted within specific research protocol seeking data. Secure encrypted email and file transfers.
Other Federal Agencies.	Joint Research Studies; Development of Government Programs; VA-	• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number(s) • Current Medications • Previous Medical History • Race/Ethnicity	34VA10 RU#1, *6, #7 HIPAA Privacy Rule (45 CFR 164.512(i) and (k))	As noted within specific research protocol seeking data. Secure encrypted

	Approved Research	• VA Research-related data	MOU	email and file transfers.

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: There is a risk of impermissible disclosure, i.e., legal authority is not present, associated with sharing information outside of VA.

Mitigation: An approved IRB protocol has been received outlining the data to be obtained along with Privacy Officer review for a determination that legal authority exists prior to disclosure.

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.

MVP has a HIPAA waiver to collect limited information for recruitment purposes only without notifying the individual. Prior to collecting and using PHI for research purposes, the individual is provided notice through the informed consent process in which they sign a consent and HIPAA authorization form. The Department of Veterans Affairs does provide public notice that the system does exist in many different ways.1. Notice is given to individuals prior to data going into the RNE application. The Office of Research and Development (ORD) provides policy guidance on how individuals are to be recruited and provided informed consent to participate in research studies in VHA Directive 1200, Research and Development Program, and corresponding Handbooks. More information on ORD can be found at: http://www.research.va.gov/.Notice of collection for research studies is recorded on the informed consent form (VA Form 10-1086). The template for VA Form 10-1086 can be found at: http://vaww.va.gov/vaforms/medical/pdf/vha-10-1086.pdf.2. VA has published in the Federal Register the Privacy Act Systems of Records Notice (SORN) SORN 34VA10, Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA. This SORN can be found online at https://www.gpo.gov/fdsys/pkg/FR-2010-05-27/pdf/2010-12758.pdf.3. This Privacy Impact Assessment (PIA) also serves as notice of the RNE application. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."4. VHA Notice of Privacy Practice is given to all enrolled Veterans every three years, upon request or when there is a significant change to the Notice. A copy of the Notice of Privacy Practices is available online at http://www.va.gov/health/
.

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

There is an approved HIPAA waiver with the VA Central IRB for purposes of recruitment only, i.e. contact information to reach out to Veterans. None of that data can be used at an individual level for research purposes until the individual signs the consent form/HIPAA authorization.

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.

The informed consent process informs the individual of what kinds of data will be collected and how it will be used and protected. See attached Informed Consent and HIPAA Authorization documents.

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

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

The MVP Patient Recruitment and Enrollment System (RNE) is a completely volunteer program for military veterans. There is no penalty or denial of service if a Veteran elect not to participate in the program. VHA Handbook 1605.01 Privacy and Release Information', paragraph n 5 refers to Patient Rights, as well as paragraph 11 refers to requests for VHA to restrict the uses and/or disclosures of the individual's individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)). 18As part of informed consent, a Privacy Notice or Confidentiality explanation is provided to active participants of VA research studies. If a participant in a research study declines to provide information the participant may not be eligible to continue to participate in the research study. In accordance with VHA Handbook 1200.05, a written HIPAA authorization signed by the individual to whom the information or record pertains or an Institutional Review Board (IRB) approved waiver of HIPAA Authorization is required when VA health care facilities need to utilize individually identifiable health information for the purpose of research. (VHA Handbook 1605.01).

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.

While individuals may have the ability to consent to various uses of their information at the VA Medical Center at the point of information collection, individuals do not have the ability to consent to the use of their information in CDW. Individuals do have the right to request access or use of their IIHI/PHI to be restricted under the HIPAA Privacy Rule. VA is not required to agree to this restriction depending on the facts and situation. As part of informed consent individuals do have the ability to consent to the use of their data in VINCI or any other IT system for a specific research project for which they are a subject. This informed consent would be for the use of all data needed for that specific research study. All participants have their rights and benefits explained to them by VA research staff prior to providing information for the study.

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?

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 members of the general public may not know that RNE exists within the Department of Veterans Affairs despite public publication of information. Additionally, there is a risk that Veterans were not given adequate notice their information was collected for use.

Mitigation: The VA mitigates this risk of not providing adequate notice to the public in two ways, as discussed in detail in question 6.1 above, the PIA and SORN are published to notify and inform the public that information collected by the VA.
Active participants in research studies are given notice and informed consent documents prior to their information being collected for the study.
Notice of collection for research studies is recorded on the informed consent form (VA Form 10-1086). The template for VA Form 10-1086 can be found at:
http://vaww.va.gov/vaforms/medical/pdf/vha-10-1086.pdf

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.

Individuals do not have access to their information save through the Freedom of Information Act (FOIA) request process.

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.***

MVP has a call center to answer any questions about the program that the public or individuals enrolled into the program have 1-866-441-6075 AskMVP@va.gov

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 exempt.

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.

Individuals may obtain copies of their consent form, HIPAA, and surveys they provided.

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.

As research data that does not impact an individual's access to federal benefits or care, the program relies on the VA quality control methods for ensuring that data accessed from those sources is accurate and corrected as needed. Self-reported data is not subject to correction. If individuals have complaints about the program, those are addresses on an individual bases, including withdrawing the individual from the program, if requested. All complaints are reported to the VA Central IRB.

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 wishing to obtain more information about access should may write or call the Director of Operations, Research and Development (12), Department of Veterans Affairs, 810 Vermont Ave., NW. Washington, DC 20420 as directed in the Privacy Act System of Record Notice (SORN) 34VA10 Veteran, Patient, Employee, and Volunteer Research and Development Project Records—VA. This SORN can be found online at http://www.gpo.gov/fdsys/pkg/FR-2004-04-07/pdf/04-7821.pdf .The procedure outlined in the SORN complies with VHA Handbook 1605.01, Paragraph 7 and VA Regulation 38 CFR § 1.577.

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 RNE 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.

System Administrators create user accounts; assign user roles: Call Center Representative, Coordinators, Read Only Users, Guest, Power User, Tester, User.

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 outside of the VA that will have access to the Patient Recruitment and Enrollment system.

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 Administrators create user accounts; assign user roles:• Admin – create user accounts, assign user roles, assign user sites as needed, manage site closures, activate and deactivate users, setup new sites edit all site information, view and edit past/present document versions, perform all task comprised within 'Call Center Representative' and 'Coordinator' roles.• Call Center Representative - • Coordinators• Read Only Users• Guest• Power User• Tester• User. Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls. OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring is performed through the use of Talent Management System (TMS).

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

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

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

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

The VA requires researchers to undergo annual trainings in research ethics, HIPAA and security. These trainings are provided via the online CITI program as well as the VA's Talent Management System (TMS). VA workforce members, including contractors, will be required to take the VA Privacy and Information Security Awareness Training and Rules of Behavior (VA10176) and the Privacy and HIPAA Focused Training (VA10203). If needed, researchers may also meet with the VA's National Center for Ethics in Health Care. In order to access the system, researchers must also undergo "MVP Patient Recruitment and Enrollment Coordinator User Training" provided by VA RNE staff. They must also adhere to the MVP rules of conduct.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* July 6, 2022
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* September 14, 2022
5. *The Authorization Termination Date:* March 8, 2023
6. *The Risk Review Completion Date:* Sept 28, 2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

N/A

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)*

No

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.*

Please provide response 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.

Please provide response 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.

Please provide response 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).

Please provide response 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
UL	**Use Limitation**

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

Signature of Responsible Officials

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

Digitally signed by Kimberly E. Murphy 183320
Date: 2023.01.26 11:37:45 -05'00'

Privacy Officer, Kimberly Murphy

Andre L. Davis 1130018

Digitally signed by Andre L. Davis 1130018
Date: 2023.01.26 09:21:33 -06'00'

Information Systems Security Officer, Andre Davis

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2023.03.16 15:32:46 -05'00'

Information Systems Owner, Christopher Brown

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

The SORN is **34VA10**, Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA. This SORN can be found online at https://www.gpo.gov/fdsys/pkg/FR-2010-05-27/pdf/2010-12758.pdf.3

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