Privacy Impact Assessment for the VA IT System called:

VA REDCap

Veterans Health Administration (VHA)

VA Office of Research and Development (ORD)

eMASS ID: 1809

Date PIA submitted for review:

14 February 2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Michelle Christiano	michelle.christiano@va.gov	706-399-7980
Information System Security Officer (ISSO)	Erick Davis	erick.davis@va.gov	512-326-6178
Information System Owner	Dr. Maria Souden	maria.souden@va.gov	708-202-2476

Abstract

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

VA REDCap (Research Electronic Data Capture) is an instance of REDCap that is installed within the Veterans Affairs Enterprise Cloud – AWS environment. VA REDCap is a secure web application for building and managing online surveys and databases for the VA. While VA REDCap is specifically geared to support data collection, it may also contain some data found elsewhere. VA REDCap supports research at the VA by allowing researchers to build online surveys and databases quickly, share projects with research team members, and export data for analysis.

Overview

The overview is the most important section of the Privacy Impact Assessment (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 business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*

VA (Veterans Affairs) REDCap (Research Electronic Data Capture) is a web-based application within the VA firewall for data collection. VA REDCap is provided by the VA Office of Research and Development (ORD) to support its mission of improving Veterans' lives through health care research. VA REDCap supports research at the VA by allowing researchers to build online surveys and databases quickly, share projects with research team members, and export data for analysis.

B. *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

Office of Research and Development (ORD)

2. *Information Collection and Sharing*

C. *Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*

It is impossible to calculate the number of individuals (research subjects) whose information is stored in VA REDCap because there is not a unique participant identifier across studies and some research projects collect data anonymously. The VA REDCap system currently has more than a million records across 15,437 projects. Based on the number of recruited participants in the largest study that may use VA REDCap, we estimate that 825,000 Veterans could have information stored in the system. Data in VA REDCap may also be about a program or feedback from VA employees.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☒	VA Employees
☒	Clinical Trainees
☒	VA Contractors
☐	Members of the Public/Individuals
☒	Volunteers

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

VA REDCap enables users to quickly develop surveys and databases from conception to production on the VA intranet without additional software requirements. This tool helps researchers enter, store, and manage their project data in a systematic manner. VA REDCap allows for easy creation of online databases and surveys without requiring knowledge of programming languages. Users can collect real time survey data from multiple VA Intranet sites by posting a link to their VA REDCap survey so that respondents within the VA network can complete the VA REDCap survey through any web browser without additional software. VA REDCap users can build forms to capture any kind of data they want. In one aspect, a VA REDCap project is like a Microsoft Excel workbook in that a user is free to enter and export anything and everything they wish into an Excel workbook. However, VA REDCap has numerous benefits over Excel for research data collection, including but not limited to: 1) an intuitive interface for data entry (with data validation); 2) encryption between the data entry client and the server; 3) audit trails for tracking data manipulation and export procedures; 4) automated export procedures; and 5) advanced features, such as branching logic, calculated fields, and data quality checks.

The data to be entered into VA REDCap depends on the data collection needs of each VA REDCap project, and VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing Institutional Review Board (IRB) for research projects and as defined by their VA chain of command for operational projects. The legal authority to collect the data and the potential magnitude of harm from any unauthorized disclosure of data is different for each project.

E. *What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.*

Information is not directly shared with any other IT system within or outside the VA intranet. However, users can import data as a comma delimited text file and export data to other programs for analysis such as Microsoft Excel, SPSS, SAS, R, or Stata. Data import and export rights are granted to specific users of each project and limited to the variables defined in the data dictionary for that project. VA REDCap users can print any data they have permission to view and export any data they have permission to export. When a user chooses to export data from VA REDCap, they can customize what they want to include in the exports, choosing as much or as little information as they like, limited to the data elements in the project that the individual user has permission to export. We cannot give a list of which data elements users export because data elements and user rights are unique to each project and user of the project.

F. Are the modules/subsystems only applicable if information is shared?

VA REDCap information is not shared.

G. *Is the system operated in more than one site to include primary and secondary 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?*

VA REDCap is a national system. VA REDCap data collection and management projects rely on a thorough study-specific data dictionary defined in an iterative self-documenting process. This means that a user creates a study project in VA REDCap by themselves based on their own needs, and VA REDCap keeps a record of every change and addition they make to their project. REDCap software was developed specifically around HIPAA-Security guidelines, and it includes a project-specific user rights management system administered by the Project Owner or Principal Investigator responsible for the project. The Project Owner or Principal Investigator can determine who has access to the project and may restrict a user to see only certain parts of a project, for example so that research assistants may see certain data for the research project but not data about whether the participant is receiving a placebo or the study drug. Data Access Groups may be defined for multi-site studies to separate the data by site of care.

3. Legal Authority and System of Record Notices (SORN)

H. *What is the citation of the legal authority?*

VIReC and Vanderbilt University executed a valid end-user license agreement, which permits the VA to use the REDCap software. Vanderbilt only allows access to their REDCap software for non-profit entities that agree to sign a license agreement. If someone installs REDCap software without signing a license agreement with Vanderbilt, that person does not have the legal authority to do so, and they are violating the law. VIReC signed a license agreement with Vanderbilt, so we are legally allowed to install REDCap software. Vanderbilt University does not have access to the VA REDCap system or any data within, nor do they provide technical support to the VA. Title 38, United States Code, Section 7301.

I. What is the SORN?

34VA10/86 FR 33015 / Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA
https://www.govinfo.gov/content/pkg/FR-2021-06-23/pdf/2021-13141.pdf

J. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

No

4. System Changes

K. Will the business processes change due to the information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

I. Will the technology changes impact information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

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 Information 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
☒ **Full** Social Security Number
☒ **Partial** 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
☒ Sex
☒ Integrated Control Number (ICN)
☒ Military History/Service Connection
☐ Next of Kin
☒ Date of Death
☐ Business Email Address
☐ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (List Below)

Other PII/PHI data elements: Dates of care, images (photograph, diagnostic image), geographic data, biometric identifiers, Any unique identifying number or code.

The authority for gathering information varies by project, as described in other items.

1.2 List 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?

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

VA REDCap creates information in the sense that it is used to electronically collect data that may not exist elsewhere. VA REDCap is available on the VA Intranet and provides functionality to manage participant enrollment, randomization, and drug or device assignment. Sources for the information in the system includes VA researchers, researchers conducting research-related work with the VA, and VA patients. VA employees logged into VA REDCap may import data into a project or enter data into a project. VA employees without VA REDCap accounts may enter data into a VA REDCap survey form. If a VA patient is using a device connected to the VA network, the VA patient may enter data into a VA REDCap survey form. Research data are entered by VA employees and/or patients only if they have been approved to collect the data by the appropriate IRB. Based on the primary data collection needs of the individual project, the system may also be used to collect data on VA contractors, volunteers, or clinical trainees.

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.

We cannot give a list of which data sources are used because data elements and sources are unique to each project and the legal authority to collect the data for the project. The data to be entered into VA REDCap depends on the data collection needs of each VA REDCap project, and VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects. The legal authority to collect the data and the potential magnitude of harm from any unauthorized disclosure of data is different for each project Information is not directly shared with any other IT system within or outside the VA intranet. However, users can import data as a comma delimited text file and export data to other programs for analysis such as Microsoft Excel, SPSS, SAS, R, or Stata. Data import and export rights are granted to specific users of each project and limited to the variables defined in the data dictionary for that project. VA REDCap users can print any data they have permission to view and export any data they have permission to export. When a user chooses to export data from VA REDCap, they can customize what they want to include in the exports, choosing as much or as little information as they like, limited to the data elements in the project that the individual user has permission to export.

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

Yes. VA REDCap is used for primary data collection. .

1.3 Methods of information collection

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

Information obtained directly from patients, employees, and/or other members of the public may be collected using either paper forms or verbally via interviews and assessments that are entered into the VA REDCap project by a VA employee. VA employees logged into VA REDCap may import data into a project or enter data into a project. VA employees without VA REDCap accounts may enter data into a VA REDCap survey form. If a VA patient is using a device connected to the VA network, the VA patient may enter data into a VA REDCap survey form. Research data are entered by VA employees and/or patients only if they have been approved to collect the data by the appropriate IRB. The legal authority to collect the data and the potential magnitude of harm from any unauthorized disclosure of data is different for each project.

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?

We cannot give a list of which data sources are used because data elements and sources are unique to each project and the legal authority to collect the data for the project. Data sources and types of information vary by project, as determined by each project owner. The data to be entered into VA REDCap depends on the data collection needs of each VA REDCap project, and VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects. If information to be entered into VA REDCap is collected on a form that is subject to the Paperwork Reduction Act, the project owner is responsible for obtaining an OMB control number, agency form number, and following the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects.

1.4 Information checks for accuracy, and 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.

Depending on the individual research study, data may be checked by audits, manual verification, and by employing field validation rules. VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects.

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?

VA REDCap does not connect to or interface with any other information systems.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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

In addition to Title 38, United States Code, Section 7301, VIReC and Vanderbilt University executed a valid end-user license agreement, which permits the VA to use the REDCap software. Vanderbilt only allows access to their REDCap program for non-profit entities that agree to sign a license agreement. If someone installs REDCap without signing a license agreement with Vanderbilt, that person does not have the legal authority to do so, and they are violating the law. VIReC signed a license agreement with Vanderbilt, so we are legally allowed to install REDCap.

The data to be entered into VA REDCap depends on the data collection needs of each VA REDCap project, and VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects. The legal authority to collect the data and the potential magnitude of harm from any unauthorized disclosure of data is different for each project.

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

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

<u>Principle of Purpose Specification:</u> The collection ties with the purpose of the underlying mission of the organization and its enabling authority.

<u>Principle of Minimization:</u> The information is directly relevant and necessary to accomplish the specific purposes of the program.

<u>Principle of Individual Participation:</u> The program, to the extent possible and practical, collects information directly from the individual.

<u>Principle of Data Quality and Integrity:</u> VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.

This 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: Some, but not all, VA research projects may collect some types of SPI. If this information was breached or accidently released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and aid the affected parties so that they may find the help they need to get through their crisis. All VA employees and contractors must complete annual Privacy and HIPAA training and VA Privacy and Security Awareness and Rules of Behavior training.

VA REDCap employs a variety of security measures designed to ensure that the information is appropriately disclosed or released. VA REDCap uses encryption in during transmission and encryption at rest. VA REDCap provides the following system level access controls:

Data Entry Rights: Grants user “No Access”, “Read Only”, “View & Edit”, or “Edit Survey Responses” rights to the project’s data collection instruments.

Manage Survey Participants: Grants user access to manage the public survey URLs, participant contact lists, and survey invitation log.

Calendar: Grants user access to track study progress and allows user to update calendar events, such as mark milestones, enter ad hoc meetings.

Data Export Tool: Grants user “No Access”, “De-identified Only” or “Full Data Set” access to export all or selected data fields to one of the 5 default programs in REDCap (SAS, SPSS, R, Stata, Excel). Default Access: De-Identified; De-identified access shifts all dates even if they are not marked as identifiers. Non-validated text fields and note fields (free text) are also automatically removed from export.

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.

PII/PHI Data Element	Internal Use	External Use

Name	Used to identify the patient during appointments and patients and employees in other forms of communication	Not used
Full Social Security Number	Used as a patient identifier	Not used
Date of Birth	Used to identify age and confirm patient identity	Not used
Mother’s Maiden Name	Used to confirm patient identity	Not used
Personal Mailing Address	Used for communication, billing purposes and calculate travel pay	Not used
Personal Phone Number(s)	Used to confirm patient identity or for communication	Not used
Personal Email Address	Used to verify the identity of the veteran who is being reviewed or for communication	Not used
Emergency Contact Information	Used for emergency contact information if necessary	Not used
Financial Information	Used for patient demographic information	Not used
Health Insurance Beneficiary Numbers Account Numbers	Used in cases of emergent situations such as medical emergencies	Not used
Integrated Control Number (ICN)	Used to confirm patient identity	Not used
Date of Death	Identifying the date of participant death if applicable.	Not used
Medications	Used to evaluate research hypotheses	Not used
Medical Records	Used to evaluate research hypotheses	Not used
Race/Ethnicity	Used for patient demographic information and for indicators of ethnicity-related diseases	Not used
Medical Record Number	Used to confirm patient identity	Not used
Sex	Used to identify study cohort, or to evaluate research hypothesis	Not used
Dates of care	Used to identify study cohort, or to evaluate research hypothesis	Not used
Images (photograph, diagnostic image)	Used to evaluate research hypothesis	Not used
Geographic data	Used to evaluate research hypothesis	Not used
Biometric identifiers	Used to identify study cohort, or to evaluate research hypothesis, or used as patient identifier	Not used
Any unique identifying number or code	Used to identify study cohort, or to evaluate research hypothesis, or used as patient identifier	Not used

2.2 Describe the types of tools 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?*

VA REDCap does not perform complex analytical tasks. Information is not directly shared with any other information technology (IT) system within or outside the VA intranet. However, users can import data as a comma delimited text file and export data to other programs for analysis such as Microsoft Excel, R programing language, or statistical analysis programs (SPSS, SAS, or Stata). Data import and export rights are granted to specific users of each project and limited to the variables defined in the data dictionary for that project. VA REDCap users can print any data they have permission to view and export any data they have permission to export. When a user chooses to export data from VA REDCap, they can customize what they want to include in the exports, choosing as much or as little information as they like, limited to the data elements in the project that the individual user has permission to export. We cannot give a list of which data elements users export because data elements and user rights are unique to each project and user of the project.

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.

Data collected in VA REDCap for a research project are not automatically entered into patient records and can only be viewed by study personnel approved by the appropriate IRB. Use of the data is governed by the research protocol approved by the appropriate IRB. VA REDCap is not to be used as a system of records (SOR) for operational purposes. There are cases where VA REDCap is used for an operational purpose, but none of the data in the project is considered a record (and therefore system of records requirements do not apply). Users are referred to their local Records Officers for questions about SOR determinations and requirements.

2.3 How the information in the system is 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?

VA REDCap RDS database encrypts the data using keys managed by the AWS Key Management Service (KMS). VA REDCap RDS database data stored at rest in the underlying storage is encrypted, as are its automated nightly backups, read replicas, and snapshots. Amazon RDS encryption uses the industry standard AES-256 encryption algorithm to encrypt data on the server that hosts the REDCap RDS instance.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

MySQL Database is encrypted with FIPS 140-2 compliant algorithms.

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

Encrypted communications between REDCap application and RDS database uses SSL/TLS. The REDCap RDS database has an SSL certificate installed.

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?

Within VA REDCap, users must be added to a specific project by the project owner or manager. All VA REDCap users are expected to abide by the regulatory, ethical, privacy and confidentiality responsibilities appropriate to their projects. For example, persons may only be added to a research project if they are listed as research personnel on the project's IRB approved protocol documents.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

VA REDCap account login is available through the VA Intranet only. Within the VA, users need to have an account made for them in the VA REDCap application. Being a VA employee does not by itself allow access to the VA REDCap application. Survey respondents can use a VA REDCap survey link from any internet-connected device, but the access is limited to submitting a survey response. Access Control policies are included in the EMASS documentation used in the VA OI&T system authorization process for the VA REDCap system https://va.emass.apps.mil/App/CA/SystemMain/1809 (accessing the link requires an EMASS account in good standing with permission to view the VA REDCap system record).

2.4c Does access require manager approval?

Within VA REDCap, users must be added to a specific project by the project owner or manager. All VA REDCap users are expected to abide by the regulatory, ethical, privacy and confidentiality responsibilities appropriate to their projects. For example, persons may only be added to a research project if they are listed as research personnel on the project's IRB approved protocol documents.

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

Each VA REDCap project has a log that tracks all activities within a project, including page views. VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects. Each VA REDCap project must have a designated Project Owner or Principal Investigator who owns the project and is responsible for meeting all regulatory and policy requirements for the project, including controlling access to and monitoring appropriate use of any PHI or PII within the project.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

Data sources and types of information vary by project, as determined by each project owner. The data to be entered into VA REDCap depends on the data collection needs of each VA REDCap project, and VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects. VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects.

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

All information entered into VA REDCap is stored indefinitely until a user or Principal Investigator specifically requests to have it deleted. The legal authority to collect the data and the obligations for record retention or destruction differ by project. VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects.

Individual projects in VA REDCap may collect all, some, or none of the following SPI: Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address, Zip Code, Personal Phone Number(s), Personal Fax Number, Personal Email Address, Emergency Contact Information (Name, Phone Number, etc., of a different individual), Current Medications, Previous Medical Records, Race/Ethnicity. VA REDCap cannot collect IP addresses. The data to be entered into VA REDCap depends on the data collection needs of each VA REDCap project, and VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects. The legal authority to collect the data and the potential magnitude of harm from any unauthorized disclosure of data is different for each project.

3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods***.** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

Each VA REDCap project must have a designated Project Owner or Principal Investigator who owns the project and is responsible for meeting all regulatory and policy requirements for the project, including requirements for data collection, data retention, and data destruction. All VA REDCap users are referred to their local Records Officer for questions about records determinations and requirements. For example, research records will be retained/destroyed in accordance with VHA Record Control Schedule (RCS 10-1) and research investigator files are covered under item number 8300.6 in the Record Control Schedule (RCS) 10-1- Temporary with cutoff at the end of the fiscal year after completion of the research project and destroy 6 years after cutoff unless the records need to be retained longer (e.g., if required by other Federal regulations or the European General Data Protection regulations). Each VA REDCap Project Owner or Principal Investigator is responsible for understanding and complying with the requirements for data collection, data retention, and data destruction appropriate for their project.

All information entered into VA REDCap is stored indefinitely until a user specifically requests to have it deleted. When a user deletes a specific piece of information or an entire record, the data is still saved in VA REDCap's robust logging feature. When a user wants to delete an entire research project, they request that from VA REDCap support team. If that project was a learning project containing "dummy data" in order to learn how to use the system, the data are deleted. If that project contains actual research data that needs to be retained, the project may be archived. Archived projects are available as "read only", meaning a user can access the data but cannot modify or delete it. The legal authority to collect the data and the obligations for record retention or destruction differ by project.

VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects.

3.3 The retention schedule 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. Please work with the system 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?

The legal authority to collect the data and the obligations for record retention or destruction differ by project. Each VA REDCap project must have a designated Project Owner or Principal Investigator who owns the project and is responsible for meeting all regulatory and policy requirements for the project, including requirements for data collection, data retention, and data destruction. All VA REDCap users are referred to their local Records Officer for questions about records determinations and requirements. For example, research records will be retained/destroyed in accordance with VHA Record Control Schedule (RCS 10-1) and research investigator files are covered under item number 8300.6 in the Record Control Schedule (RCS) 10-1- Temporary with cutoff at the end of the fiscal year after completion of the research project and destroy 6 years after cutoff unless the records need to be retained longer (e.g., if required by other Federal regulations or the European General Data Protection regulations). Each VA REDCap Project Owner or Principal Investigator is responsible for understanding and complying with the requirements for data collection, data retention, and data destruction appropriate for their project.

All information entered into VA REDCap is stored indefinitely until a user specifically requests to have it deleted. When a user deletes a specific piece of information or an entire record, the data is still saved in VA REDCap's robust logging feature. When a user wants to delete an entire research project, they request that from VA REDCap support team. If that project was a learning project containing "dummy data" in order to learn how to use the system, the data are deleted. If that project contains actual research data that needs to be retained, the project may be archived. Archived projects are available as "read only", meaning a user can access the data but cannot modify or delete it. The legal authority to collect the data and the obligations for record retention or destruction differ by project.

VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects.

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

Each VA REDCap project must have a designated Project Owner or Principal Investigator who owns the project and is responsible for meeting all regulatory and policy requirements for the project, including requirements for data collection, data retention, and data destruction. All VA REDCap users are referred to their local Records Officer for questions about records determinations and requirements. For example, research records will be retained/destroyed in accordance with VHA Record Control Schedule (RCS 10-1) and research investigator files are covered under item number 8300.6 in the Record Control Schedule (RCS) 10-1- Temporary with cutoff at the end of the fiscal year after completion of the research project and destroy 6 years after cutoff unless the records need to be retained longer (e.g., if required by other Federal regulations or the European General Data Protection regulations). Each VA REDCap Project Owner or Principal Investigator is responsible for understanding and complying with the requirements for data collection, data retention, and data destruction appropriate for their project.

All information entered into VA REDCap is stored indefinitely until a user specifically requests to have it deleted. When a user deletes a specific piece of information or an entire record, the data is still saved in VA REDCap’s robust logging feature. When a user wants to delete an entire research project, they request that from VA REDCap support team. If that project was a learning project containing “dummy data” in order to learn how to use the system, the data are deleted. If that project contains actual research data that needs to be retained, the project may be archived. Archived projects are available as “read only”, meaning a user can access the data but cannot modify or delete it. The legal authority to collect the data and the obligations for record retention or destruction differ by project.

VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects.

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.

Each VA REDCap project must have a designated Project Owner or Principal Investigator who owns the project and is responsible for meeting all regulatory and policy requirements for the project, including requirements for data collection, data retention, and data destruction. All VA REDCap users are referred to their local Records Officer for questions about records determinations and requirements. For example, research records will be retained/destroyed in accordance with VHA Record Control Schedule (RCS 10-1) and research investigator files are covered under item number 8300.6 in the Record Control Schedule (RCS) 10-1- Temporary with cutoff at the end of the fiscal year after completion of the research project and destroy 6 years after cutoff unless the records need to be retained longer (e.g., if required by other Federal regulations or the European General Data Protection regulations). Each VA REDCap Project Owner or Principal Investigator is responsible for understanding and complying with the requirements for data collection, data retention, and data destruction appropriate for their project.

All information entered into VA REDCap is stored indefinitely until a user specifically requests to have it deleted. When a user deletes a specific piece of information or an entire record, the data are still saved in VA REDCap's robust logging feature. When a user wants to delete an entire research project, they request that from VA REDCap support team. The legal authority to collect the data and the obligations for record retention or destruction differ by project. VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects.

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.

VA REDCap implements four controls to protect PII used within VA REDCap projects:

1) VA REDCap login is only accessible from the VA intranet, so individuals must have a PIV card and VA network access to reach the application.
2) Within the VA, users need to have an account made for them in VA REDCap. Being a VA employee does not by itself allow access to VA REDCap.
3) Within VA REDCap, users must be added to a specific project by the project owner or their designee.
4) Within a VA REDCap project, the project owner can restrict which users have access to which data based on their project roles. If a user is found to be inappropriately using information, they may be banned from the specific project or from VA.

<u>3.6 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 Privacy Officer (PO) to complete all Privacy Risk questions inside the document in 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: *The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.*

Principle of Data Quality and Integrity: *The PIA should describe 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 VA REDCap 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: Each VA REDCap project must have a designated Project Owner or Principal Investigator who owns the project and is responsible for meeting all regulatory and policy requirements for the project, including requirements for data collection, data retention, and data destruction. All VA REDCap users are referred to their local Records Officer for questions about records determinations and requirements.

To mitigate the risk posed by information retention, VA REDCap uses encryption in transmission and encryption at rest. By default, VA REDCap data are kept indefinitely in accordance with the General Records Schedule 20, approved by National Archives and Records Administration (NARA). All information entered in VA REDCap is stored indefinitely until a user specifically requests to have it deleted. When a user deletes a specific piece of information or an entire record, the data are still saved in VA REDCap's robust logging feature. When a user wants to delete an entire research project, they request that from VA REDCap support team.

When data are entered into VA REDCap for research purposes, research records will be retained/destroyed in accordance with VHA Record Control Schedule (RCS 10-1) and research investigator files are covered under item number 8300.6 in the Record Control Schedule (RCS) 10-1- Temporary with cutoff at the end of the fiscal year after completion of the research project and destroy 6 years after cutoff unless the records need to be retained longer (e.g., if required by other Federal regulations or the European General Data Protection regulations).

The legal authority to collect the data and the obligations for record retention or destruction differ by project. VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a VA REDCap consists of six 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 VA REDCap 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 3.9a 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
AWS Production Web Server (Apache)	No	No	None	N/A	HTTPS encryption, HTTP Strict Transport Security (HSTS)
EC2 Instance Autoscaling	No	No	None	N/A	None
Red Hat Linux 8 Operating System	No	No	None	N/A	Secure Configuration using STIGs/SRGs
Amazon RDS (MySQL Community)	Yes	Yes	Name, Full Social security number, date of birth, mother’s maiden name, personal mailing address, personal phone number(s), personal email address, emergency contact information,	Database stores PII/PHI	Secure Configuration, encryption with FIPS 140 -2 compliant algorithms

			current medications, previous medical records, race/ ethnicity, Dates of care, images (photograph, diagnostic image), geographic data, biometric identifiers, Any unique identifying number or code		
Vanderbuit REDCap Application	Yes	No	Name, Full Social security number, date of birth, mother’s maiden name, personal mailing address, personal phone number(s), personal email address, emergency contact information, current medications, previous medical records, race/ ethnicity, Dates of care, images (photograph, diagnostic image), geographic data, biometric identifiers, Any unique identifying number or code	Researchers seek PII in conjunction with the creation of survey questionnaires	Session timeout, role based access, audit logging, industry standard application security, data gets intentionally filtered, sanitized, data type checking, and escaped which protect against methods of attack, such as Cross-Site Scripting (XSS) and SQL Injection
PHP Programming Language	No	No	None	N/A	None

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Any VA Program Office	Data can be shared with other VA REDCap users based on their project/user permissions	Name, Full and/or Partial 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, Financial Information, Health Insurance Beneficiary Numbers, Sex, Integrated Control Number (ICN), Date of Death, current medications, previous medical records, race/ethnicity, dates of care,	Within the VA REDCap application by sharing permission. Users with permission on a project to download data may download data files.

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
		images (photograph, diagnostic image), geographic data, biometric identifiers, any unique identifying number or code	

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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

Follow the format below:

Privacy Risk: VA REDCap does not connect to other organizations and does not share any information with other information systems. VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects. As with any system, there is a risk that sharing data within the Department of Veterans' Affairs could happen and the data may be disclosed to individuals who do not require access, which heightens the threat of the information being misused.

Mitigation: VA REDCap uses encryption in transmission and encryption at rest. The principal of need-to-know is strictly adhered to by the VA REDCap personnel. Being a VA employee does not by itself allow access to VA REDCap or a particular VA REDCap project. Each VA REDCap project must have a designated Project Owner or Principal Investigator who owns the project and meets key responsibilities, including managing project roles and permissions of team members within the VA REDCap project with the User Rights and Data Access Groups tools. In rare instances when the VA REDCap project owner is no longer working at the VA and did not transfer rights to the new project owner, the VA REDCap Project Manager will assign rights to the project for the new project owner. Additionally, VA employees undergo annual Privacy/HIPAA (Health Insurance Portability and Accountability Act) training and Privacy and Security Awareness and Rules of Behavior training. VA employees utilize secure passwords, personal identification verification (PIV) cards, and personal identifiable numbers (PIN).

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

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

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

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: N/A there are no direct links or interfaces between VA REDCap and any other information system.

Mitigation: N/A there are no direct links or interfaces between VA REDCap and any other information system.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.
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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

The VA provides effective notice to individuals and the public regarding activities that impact privacy, collection (including PII), use, sharing, safeguarding, maintenance, and disposal of PII. VA approved forms, which collect PII/PHI, have the Privacy Act statement prominently displayed at the top of the form. Any non-VA approved form, which collects PII/PHI, is to be approved by the VA REDCap PO, at which time the form will be reviewed for the requirement of the Privacy Act statement.

6.1b If notice was not provided, explain why.

As described previously, data sources and types of information vary by project, including the Notice of Privacy Practices (NOPP) and SORN that is applicable. The NOPP for the specific research project will vary, but VA publication 10-163 Notice of Privacy Practices is used for all persons receiving care from VHA. Veterans are provided the NOPP on a triennial basis. Others are provided the NOPP when the VA provides an episode of care."

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=8928

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

Data sources and types of information vary by project, as determined by each project owner. The data to be entered into VA REDCap depends on the data collection needs of each VA REDCap project, and VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects. VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects. For research projects, the IRB also approves a protocol by which informed consent to participate in research is obtained from individuals, or an approval to waive informed consent with a justification (for example, the usual process to obtain informed consent would identify the individual and the fact of their participation in the research could identify them as an at-risk group such as illegal drug users). The IRB or Privacy Board also approves a HIPAA compliant waiver or HIPAA authorization (either a separate VA Form 10-0493 or combined with the informed consent form (ICF), when applicable) that identifies uses of PHI under the HIPAA Privacy Regulation. Therefore, waivers and how the notice is provided may vary by project. The Federal Register published a revised Federal Policy for the Protection of Human Subjects, subsequently revised January 22, 2018 and again June 19, 2018. The Department of Veterans Affairs (VA), one of 20 federal departments and agencies that follow the revised policy, known as a "Common Rule", codified the regulation as eCFR :: 38 CFR Part 16 -- Protection of Human Subjects. The Common Rule/Final Rule governs how research data is collected at VHA. Additional rules, such as Requirements for Surveys & Interviews (Projects Conducted for Research & Operational Purposes) may also apply. Project owners are responsible to know and comply with all applicable regulations and policies.

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.

Veterans or their representatives are given the Notice of Privacy Practices (NOPP) at the time of treatment with a signed acknowledgement received, which informs them of the use and disclosures and the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII. Veterans are provided the NOPP on a triennial basis. Others are provided the NOPP when the VA provides an episode of care. Research subjects that are non-Veterans will also receive the Notice of Privacy Practices and the HIPAA authorization (either a separate VA Form 10-0493 or combined with the informed consent form (ICF), when applicable) that identifies uses of PHI under the HIPAA Privacy Regulation contains the Privacy Act Statement. Participants must sign IRB approved research informed consent form (ICF) if a waiver for informed consent was not obtained from the relevant Institutional Review Board(s).

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.

The Federal Register published a revised Federal Policy for the Protection of Human Subjects, subsequently revised January 22, 2018 and again June 19, 2018. The Department of Veterans Affairs (VA), one of 20 federal departments and agencies that follow the revised policy, known as a "Common Rule", codified the regulation as eCFR :: 38 CFR Part 16 -- Protection of Human Subjects. The Common Rule/Final Rule governs how research data is collected at VHA. In cases where informed consent is waived by the appropriate IRB there is a justification, for example, that recording of the individual's consent to participate in the research itself poses a potential risk to the participant (e.g., being identified as an illegal drug user by participating in a substance use disorder study).

https://www.gpo.gov/fdsys/pkg/FR-2017-01-19/pdf/2017-01058.pdf

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 Privacy Officer (PO) 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: *This is referring to sufficient notice provided to the individual.*

Principle of Use Limitation: *The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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 veterans and other members of the public will not know that VA REDCap exists or that it collects, maintains, and/or disseminates PII, PHI, or PII/PHI about them.

Mitigation: This risk is mitigated by the informed consent process when Veterans are enrolled to participate in research projects, per VHA Directive 1200.05(4) REQUIREMENTS FOR THE PROTECTION OF HUMAN SUBJECTS IN RESEARCH and federal regulation eCFR :: 38 CFR Part 16 -- Protection of Human Subjects. All individuals involved in the conduct of VA human subjects research are required to maintain current training on these requirements and ethical principles on which human subjects research is to be conducted, regardless of pay status, appointment type, or length of time at the VA facility. This risk is also mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans are enrolled for health care. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SOR) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

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 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

- VA REDCap provides individuals the right of access, under the Privacy Act of 1974, only to their records which are not exempt pursuant to subsections (j) and (k) of the Privacy Act. Veterans may obtain medical records with a written request or on VA Form 10-5345a.
- Veterans may also view their medical records on My HealtheVet, after signing up.
- An individual wanting notification or access, including contesting the record, should mail or deliver a request to the office identified in the SORN. If an individual does not know the "office concerned," the request may be addressed to the PO or FOIA/PO of any VA field station or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420.

- VA REDCap follows the guidance of Office of Management and Budget (OMB) Circular A-130 when processing Privacy Act/FOIA requests from individuals.’
- Procedures for adhering to a FOIA request are outlined in VA Handbook 6300.4: Procedures for Processing Requests for Records Subject to the Privacy Act.
- The Federal Register published a revised Federal Policy for the Protection of Human Subjects, subsequently revised January 22, 2018 and again June 19, 2018. The Department of Veterans Affairs (VA), one of 20 federal departments and agencies that follow the revised policy, known as a “Common Rule”, codified the regulation as eCFR :: 38 CFR Part 16 -- Protection of Human Subjects. The Common Rule/Final Rule governs how research data is collected at VHA. In cases where informed consent is waived by the appropriate IRB there is a justification, for example, that recording of the individual’s consent to participate in the research itself poses a potential risk to the participant (e.g., being identified as an illegal drug user by participating in a substance use disorder study).

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)?

Varies by project. The information in VA REDCap may or may not be exempt from access provisions of the Privacy Act. Individual project owners are responsible for ensuring appropriate data access to their project, whether for purposes of complying with a FOIA request or for any other reason.

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?

Varies by project. The information in VA REDCap may or may not be exempt from access provisions of the Privacy Act. Individual project owners are responsible for ensuring appropriate data access to their project, whether for purposes of complying with a FOIA request or for any other reason.

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.

An individual may request amendment of a record pertaining to them contained in a specific VA system of records by mailing or delivering the request to the office concerned. The request must be in writing and must conform to the requirements in VA Handbook 6300.4. It must state the nature of the information in the record the individual believes to be inaccurate, irrelevant, untimely, or incomplete; why the record should be changed; and the amendment desired. The requester is advised of the title and address of the VA official who can assist in preparing the request to amend the record if assistance is desired.

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.

Within 10 business days, the requester is provided a written acknowledgement of receipt of the request and formal decisions to amend the record is provided within 30 days. Where the VA agrees with the individual's request to amend their record(s), the record(s) will be corrected promptly, and the individual will be notified of the correction.

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.

Varies by project. In cases where research data is collected anonymously, it may not be possible for an individual to correct the data after it is submitted. The Federal Register published a revised Federal Policy for the Protection of Human Subjects, subsequently revised January 22, 2018 and again June 19, 2018. The Department of Veterans Affairs (VA), one of 20 federal departments and agencies that follow the revised policy, known as a "Common Rule", codified the regulation as eCFR :: 38 CFR Part 16 -- Protection of Human Subjects. The Common Rule/Final Rule governs how research data is collected at VHA. In cases where informed consent is waived by the appropriate Institutional Review Board(s) there is a justification, for example, that recording of the individual's consent to participate in the research itself poses a potential risk to the participant (e.g., being identified as an illegal drug user by participating in a substance use disorder study).

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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
<u>Principle of Individual Participation:</u> The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

<u>Principle of Individual Participation:</u> The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.
This question is related to privacy control IP-3, Redress.

Follow the format below:

<u>Privacy Risk:</u> Varies by project. In cases where research data is collected anonymously, it may not be possible for an individual to correct the data after it is submitted. The Federal Register published a revised Federal Policy for the Protection of Human Subjects, subsequently revised January 22, 2018 and again June 19, 2018. The Department of Veterans Affairs (VA), one of 20 federal departments and agencies that follow the revised policy, known as a "Common Rule", codified the regulation as eCFR :: 38 CFR Part 16 -- Protection of Human Subjects. The Common Rule/Final Rule governs how research data is collected at VHA. In cases where informed consent is waived by the appropriate IRB there is a justification, for example, that recording of the individual's consent to participate in the research itself poses a potential risk to the participant (e.g., being identified as an illegal drug user by participating in a substance use disorder study).

<u>Mitigation:</u> Varies by project. In cases where research data is collected anonymously, it may not be possible for an individual to correct the data after it is submitted. The Federal Register published a revised Federal Policy for the Protection of Human Subjects, subsequently revised January 22, 2018 and again June 19, 2018. The Department of Veterans Affairs (VA), one of 20 federal departments and agencies that follow the revised policy, known as a "Common Rule", codified the regulation as eCFR :: 38 CFR Part 16 -- Protection of Human Subjects.The Common Rule/Final Rule governs how research data is collected at VHA. In cases where informed consent is waived by the appropriate IRB there is a justification, for example, that recording of the individual's consent to participate in the research itself poses a potential risk to the participant (e.g., being identified as an illegal drug user by participating in a substance use disorder study).

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be documented.

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

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

The data to be entered into VA REDCap depends on the data collection needs of each VA REDCap project, and VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects. The legal authority to collect the data and the potential magnitude of harm from any unauthorized disclosure of data is different for each project. VA REDCap project owners are responsible for granting appropriate access to data in their project.

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?

N/A. VHA active directory account and VA REDCap account with granted permissions are required to access data within the VA REDCap 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.

Roles and user rights vary by project. The data to be entered into VA REDCap depends on the data collection needs of each VA REDCap project, and VA REDCap users are responsible for abiding by the regulatory, ethical, privacy, and confidentiality responsibilities appropriate to their projects as defined by their overseeing IRB for research projects and as defined by their VA chain of command for operational projects. The legal authority to collect the data and the potential magnitude of harm from any unauthorized disclosure of data is different for each project. VA REDCap project owners are responsible for granting appropriate access to data in their project.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2a *Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?*

Yes.

8.2a. *Will VA contractors have access to the system and the PII?*

Yes, contractors may have access to the system. Contracts are reviewed annually at a minimum. All contractors are cleared using the VA background investigation process. The contractors are required to complete annual VA Privacy and Security Awareness and Rules of behavior training via the VA's TMS.

8.2b. *What involvement will contractors have with the design and maintenance of the system?*

Contractors who are authorized privileged access to the VA REDCap provide critical technical support and maintenance to ensure the operational confidentiality, Integrity, and availability of the information system.

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.

Individuals who provide support to the system are required to complete annual VA Privacy and Security Awareness and Rules of Behavior training via Talent Management System (TMS). Users are required to complete information system security training activities including annual security awareness training and specific information system security training. The training records are retained for 7 years. This documentation and monitoring are performed through TMS.

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If completed, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 14-Feb-2024
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 10-May-2024
5. *The Authorization Termination Date:* 10-May-2026
6. *The Risk Review Completion Date:* 08-May-2024
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 not completed 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. ***(Refer to question 1.8 of the PTA)***

VA Enterprise Cloud (VAEC), IaaS for Web Server, PaaS for Database

9.2 Does the contract with the Hosting 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 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes. Hosting Site: VAEC AWS, Contract No: ECC is NNG15SD22B / VA118-17-F-2284, VAEC AWS is a FedRAMP approved cloud service provider. All data within VA REDCap is owned by the VA, and the individual VA REDCap Project Owners are responsible for stewardship of the data within their VA REDCap projects.

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.

No

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

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

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

The roles and responsibilities are mapped out between the VAEC (Cloud provider) and the internal VA REDCap Technical Team to manage risks and ensure requirements are met. The VA REDCap Technical Team is comprised of system administrators, database administrators, security personnel, and application administrators. These are the security and privacy related tasks accomplished by each team:

Data Encryption: Provided by VAEC – All data is encrypted with FIPS 140-2 compliant hardware and certified at FIPS 140-2 Security Level 3.

NESSUS vulnerability scan – Retrieved, reviewed by the VA REDCap Technical Team, and remediated by the VAEC.

WASA/Penetration scans/testing – Requested, reviewed by the VA REDCap Technical Team, and remediated by both VAEC and VA REDCap Technical Team as applicable.

Routine ATO controls (User review, artifact creation, etc.) – Completed by the VA REDCap Technical Team.

Security Documentation (POA&Ms, eMASS, Hardware/Software list, etc.) – Completed by the VA REDCap Technical Team.

STIG Compliance: Completed by the VAEC.

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).

RPA is not being utilized for VA REDCap.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

MICHELLE CHRISTIANO

Digitally signed by MICHELLE CHRISTIANO
Date: 2025.05.29 07:05:11 -04'00'

Privacy Officer, Michelle Christiano

ERICK DAVIS

Digitally signed by ERICK DAVIS
Date: 2025.05.29 07:31:27 -05'00'

Information System Security Officer, Erick Davis

MARIA SOUDEN

Digitally signed by MARIA SOUDEN
Date: 2025.05.29 17:40:38 -05'00'

Information System Owner, Dr. Maria Souden

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).

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=8928

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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 Directive 1605.04
IB 10-163p (va.gov)