SPLASH PAGE LANGUAGE

The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements
under the Federal Information Security Management Act (FISMA).

VA HANDBOOK 6508.1: "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," July 2015, https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=810&FType=2

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Privacy Impact Assessment for the VA IT System called:

VA REDCap

Office Research and Development

VHA

Date PIA submitted for review:

10/26/2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kim Murphy	Kim.murphy@va.gov	781-331-3206
Information System Security Officer (ISSO)	Stuart Chase	Stuart.chase@va.gov	410-340-2018
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?" and will be published online to accompany the PIA link.

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 within the VA firewall. 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 PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

- VA (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.

- VA REDCap is hosted in the VA Enterprise Cloud (VAEC) and user support is provided by VA Information Resource Center (VIReC).

- 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 7,964 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.

- 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.

- 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.

- 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 study-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.

- 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.

- The completion of this PIA will not result in circumstances that require changes to business processes.

- The completion of this PIA will not result in technology changes.

- The identified SORN covers cloud usage and storage.

Section 1. Characterization of the Information

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

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

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

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

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

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

Individual projects in VA REDCap may collect all, some, or none of the above SPI. 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 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.

PII Mapping of Components

VA REDCap consists of 1 key components (databases). 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.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
REDCAPdev (preprod)	**Yes**	**Yes**	*Name, Social security number, date*	Researchers seek PII in conjunction	Database is encrypted with FIPS 140-2

			of birth, mother's maiden name, personal mailing address, personal phone number(s) personal fax number, personal email address, emergency contact information, current medications, previous medical records, race/ethnicity	with the creation of survey questionnaires	compliant algorithms
REDCAPprod (prod)	**Yes**	**Yes**	*Name, Social security number, date of birth, mother's maiden name, personal mailing address, personal phone number(s) personal fax number, personal email address, emergency contact information, current medications, previous*	Researchers seek PII in conjunction with the creation of survey questionnaires	Database is encrypted with FIPS 140-2 compliant algorithms

			medical records, race/ethnicity		

1.2 What are the sources of the information in the system?

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

1.3 How is the information collected?

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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.

1.4 How will the information be checked for accuracy? How often will it be checked?

This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

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 Institutional Review Board (IRB) for research projects and as defined by their VA chain of command for operational projects.

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

This question is related to privacy control AP-1, Authority to Collect

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 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.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:
Privacy Risk: 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:

User Right	Access
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 will be used in support of the program's business purpose.

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

The 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.

Individual research projects have individual reasons for collecting SPI to verify Veteran identity and use for correspondence with the Veteran. All SPI collection must be approved by the relevant Human Subjects Subcommittees. Common SPI data elements and possible reasons for collecting it are presented in the table below.

SPI data element	**Reason for collection**
Name	Used to identify the patient during appointments and patients and employees in other forms of communication.
Social Security Number	Used as a patient identifier.
Date of Birth	Used to identify age and confirm patient identity.
Mother's Maiden Name	Used to confirm patient identity.
Mailing Address	Used for communication, billing purposes and calculate travel pay.
Zip Code	Used as part of the mailing address.
Phone Number(s)	Used to confirm patient identity or for communication.
Fax Number	Used for communication.
Email Address	Used to verify the identity of the veteran who is being reviewed or for communication.
Emergency Contact Information (Name, Phone Number, etc. of a different individual)	Used in cases of emergent situations such as medical emergencies.
Current Medications	Used to evaluate research hypotheses.
Previous Medical Records	Used to evaluate research hypotheses.
Race/Ethnicity	Used for patient demographic information and for indicators of ethnicity-related diseases

2.2 What types of tools are used to analyze data and what type of data may be produced?

Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need

additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

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.

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.

2.3 How is the information in the system secured?

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

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

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

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

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access

documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

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

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

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

Add answer here:

VA REDCap employs four access gatekeepers to all research data.

1) VA REDCap is only accessible from the VA intranet, so individuals must have a PIV card and computer access or be using a VA device configured for a non-VA employee to use (e.g., a Veteran kiosk) for responding to surveys.
2) 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.
3) Within VA REDCap, users must be added to a specific research project by the project owner or manager. Persons may only be added to a research project if they are listed as research personnel on the project's IRB protocol documents.
4) Within a VA REDCap research project, the project manager 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 research project or from VA REDCap as a whole.

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.

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 Institutional Review Board (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 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.

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

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 Institutional Review Board (IRB) for research projects and as defined by their VA chain of command for operational projects.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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

Data are entered into VA REDCap for research purposes. Individual studies have individual data retention plans approved by their appropriate IRB. One study may require that the data is retained for 7 years, but another study may require that the data is destroyed within 1 year.
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 Institutional Review Board (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 of SPI?

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

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 Institutional Review Board (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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

VA REDCap implements four controls to protect PII used for research.

1) VA REDCap is only accessible from the VA intranet, so individuals must have a PIV card and computer access or be using a VA device configured for a non-VA employee to use (e.g., a Veteran kiosk) for responding to surveys.
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 research project by the project owner or manager. Persons may only be added to a research project if they are listed as research personnel on the project's IRB protocol documents.
4) Within a VA REDCap research project, the project manager 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 research project or from VA REDCap as a whole.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

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

Follow the format below:

Privacy Risk: 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: 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).

Data are entered into VA REDCap for research purposes. Individual studies have individual data retention plans approved by their appropriate IRB. One study may require that the data is retained for 7 years, but another study may require that the data is destroyed within 1 year. 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 Institutional Review Board (IRB) for research projects and as defined by their VA chain of command for operational projects. 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.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
N/A			

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: 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 Institutional Review Board (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 principle 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. Only personnel specifically added to a research project by the project manager in compliance with their IRB-approved protocol documents are allowed access study data in VA REDCap. 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 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

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

NOTE: Question 3.11 on Privacy Threshold Analysis should be used to answer this question.
Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

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

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

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

Data Shared with External Organizations

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

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

VA REDCap does not connect to other organizations and does not share any information.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: 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 Institutional Review Board (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 principle 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. Only personnel specifically added to a research project by the project manager in compliance with their IRB-approved protocol documents are allowed access study data in VA REDCap. 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 6. Notice

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

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

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

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

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

This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

Data are entered into VA REDCap by hundreds of distinct research teams conducting IRB-approved research. Each research protocol includes its own Privacy Policy to be given to research participants.

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

Data are entered into VA REDCap by hundreds of distinct research teams following IRB-approved research protocols. Each research protocol includes its own policies about right to decline.

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

Data are entered into VA REDCap by hundreds of distinct research teams following IRB-approved research protocols. Each IRB evaluates informed consent documents and procedures.

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

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

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

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

<u>Principle of Use Limitation:</u> Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:

Privacy Risk: There is a risk that members of the public may not know that the VA REDCap system exists within the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk by requiring all research protocols to include information about where and how their data will be stored.

Section 7. Access, Redress, and Correction

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

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

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

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

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location described in the informed consent document for the research study in which they are participating.

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.

Individuals seeking to correct inaccurate or erroneous information in this system may write, call or visit the VA facility location described in the informed consent document for the research study in which they are participating.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are informed of these procedures when they read and discuss the informed consent document for the research study in which they are participating.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Individuals have many alternatives available to gain access to their information in this system. They may write, call or visit the VA facility location described in the informed consent document for the research study in which they are participating.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that individuals may seek to access or redress records about them related to their participation in research and become frustrated with the results of their attempt.

Mitigation: By publishing this PIA, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on the VA REDCap application. Furthermore, the informed consent document for the research study in which they are participating provides the point of contact for members of the public who have questions or concerns about applications and evidence files.

Section 8. Technical Access and Security

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

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

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

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

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

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

VHA will maintain the data in compliance with applicable VA security policy directives that specify the standards that will be applied to protect sensitive personal information. Access to VA working space is restricted to VA employees on a "need to know" basis. Generally, VA computer areas are locked after normal duty hours and protected from outside access by the Federal Protective Service.

Strict control measures are enforced to ensure that disclosure is limited to a "need to know" basis. Digital research records stored in VA REDCap are accessible by authorized VA personnel via VA computers or computer systems. They are required to take annual VA mandatory data

privacy and security training. Security complies with applicable Federal Information Processing Standards (FIPS) issued by the National Institute of Standards and Technology (NIST). Contractors and their subcontractors who access the data are required to maintain the same level of security as VA staff.

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

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

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

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 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 the use of the Talent Management System (TMS)

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date, .*
6. *The Risk Review Completion Date*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

No, IOC: March 01, 2022

Section 9 – Technology Usage

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

9.1 Does the system use cloud technology?

If so, 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.

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Yes, VA REDCap utilizes VAEC AWS.

9.2 Identify the cloud model being utilized.

Example: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

IaaS for Web Server, PaaS for Database

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

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

Yes, handled through VAEC contract number for ECC is NNG15SD22B / VA118-17-F-2284

9.4 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

9.5 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 principal is described in the customer contract. The project is using VAEC as a Platform as a Service (PaaS).

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

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

N/A

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Digitally signed by Kimberly E. Murphy 183320
Date: 2021.11.23 12:02:02 -05'00'

Privacy Officer, Kim Murphy

Stuart E. Chase 3385791

Digitally signed by Stuart E. Chase 3385791
Date: 2021.12.16 10:37:22 -05'00'

Information System Security Officer, Stuart Chase

Maria Souden 744039

Digitally signed by Maria Souden 744039
Date: 2021.12.16 09:03:42 -06'00'

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).