Privacy Impact Assessment for the VA IT System called:

Qualtrics XM Platform -Enterprise

Veterans Health Administration

Office of Research and Development

eMASS ID #:0206

Date PIA submitted for review:

12/2/24

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	512-937-4550
Information System Owner	Henna Grover	Henna.Grover@va.gov	410-216-4566

Abstract

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

The Qualtrics XM survey platform (Qualtrics) provides clinical researchers with a secure, self-serviced, cloud-based research platform. Qualtrics enables users to collect, analyze, and visualize information gathered through online surveys of veterans and other research subjects. The system also provides various distribution methods to distribute surveys to survey respondents, aggregates that data in an easy-to-understand manner and allows researchers to act on the insights gained from the data. Researchers have many different options for analyzing the data within the platform and can also export the data to use a statistical analysis tool of their choice. This product will give researchers and general staff the ability to conduct secure research activities inside and outside of VA's secure environment.

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?

Qualtrics is a self-service research, analytics and reporting platform that allows clinical researchers to conduct research with veterans and providers through multiple channels (e.g., email, offline, mobile, etc.). Use of the product aligns to:

1. VA must continue to invest in groundbreaking research that contributes to the quality of life for Veterans—and for all Americans.
2. VA Strategic Goals - VA provides excellent care and services to the Veterans who courageously undertook the mantle of defense of the Nation.

a. To deliver on our priorities, VA will aggressively seize opportunities driven by rapid advancements in technology and ground-breaking research to provide Veterans cutting-edge treatment and means to access care, benefits, and services.

3. Performance Goal: VA has aligned its strategic footprint and services to ensure it can adapt quickly to changing Veteran needs.

a. VA has an extremely robust research and development capability and innovates to improve services to Veterans and employees.

4. Business Strategy: Enhance the nation's medical research and graduate medical education capability

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.

Qualtrics Experience Management Platform (Qualtrics) is VA Controlled / non-VA Owned and Operated

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?

The number of individuals with info in the system is determined by the number of product accounts purchased by ORD. The system is both purchased and managed from VACO, and smaller contracts have been initiated at the site level.

Total Internal Accounts Purchased: 1,000
Actual Number of Veteran Users: 22,791
Total Number of Anticipated Users: 1,000,000

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?*

Qualtrics provides clinical researchers with a secure, self-serviced, cloud-based research platform that enables them to collect and analyze information gathered through online surveys of veterans and other research subjects. The information in the system may include privacy-related information such as personally identifiable information (PII) as defined by the Privacy Act of 1974, information in identifiable form (IIF) as defined by the E-Government Act of 2002, and Protected Health Information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA), as well as other forms of sensitive information such as information protected by the 38 CFR Part 16 Protection of Human Subjects (e.g. The Common Rule"), controlled unclassified information (CUI), and information exempted from release under the Freedom of Information Act (FOIA). The size and amount and sensitivity of data collected by Qualtrics varies by project, but the platform is set up to allow the collection of information (survey responses) from up to millions of respondents.

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

Qualtrics provides clinical researchers with a secure, self-serviced, cloud-based research platform that enables them to collect and analyze information gathered through online surveys of veterans and other research subjects. The platform is set up to allow the collection of information (survey responses) from up to millions of respondents.

The Qualtrics system is operated at several geographically dispersed research locations throughout the VA. Because the system is web-based, management of any PII is done centrally within the VA instance of Qualtrics. ORD and its associated research programs will employ identical controls across all sites using Qualtrics. The Qualtrics platform is FedRAMP authorized.

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

Yes

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?*

The Qualtrics system is operated at several geographically dispersed research locations throughout the VA. Because the system is web based, management of any PII is done centrally within the VA instance of Qualtrics. ORD and its associated research programs will employ identical controls across all sites using Qualtrics. The Qualtrics platform is FedRAMP authorized. VA retains all ownership of data

collected by Qualtrics. “Moderate” harm would be the result of an intentional or unintentional disclosure of privacy related data.

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

H. What is the citation of the legal authority?

Title 38, United States Code, Section 7301
34VA10 “Veteran, Patient, Employee, and Volunteer Research and Development ProjectRecords—VA” Published in the “Federal Register / Vol. 86, No. 118 / Wednesday, June 23, 2021 / Notices.”

I. What is the SORN?

34VA10-Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA

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
- ☒ Gender/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: religion, pronouns, sexual orientation, preferred written language, education type, age, education level, branch of service, time served, active-duty status.

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

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?

Survey respondents are the source of information.

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.

Survey respondents are the source of information.

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

Survey respondents are the source of information, and reports are created based on that information.

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?

Qualtrics is used to create surveys that collect research relative information from research subjects. Subjects are provided with a web address link to the Qualtrics platform. The responses gathered are used to support protocol hypotheses.

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?

Information is not collected on a form and is not subject to the Paperwork Reduction Act

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.

Responses gathered from subjects are presumed to be accurate and will not be re-checked for accuracy.

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?

Responses gathered from subjects are presumed to be accurate and will not be re-checked for accuracy.

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

Title 38, United States Code, Section 7301

Responses gathered from subjects are presumed to be accurate and will not be re-checked for accuracy.

34VA10 "Veteran, Patient, Employee, and Volunteer Research and Development Project Records—VA" Published in the "Federal Register / Vol. 86, No. 118 / Wednesday, June 23, 2021 / Notices."

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: The collection ties with the purpose of the underlying mission of the organization and its enabling authority.

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

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

Principle of Data Quality and Integrity: *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:
Privacy related information is collected under legal authorities cited or referenced in the individual project/protocol. The Qualtrics platform supports VA projects as directed by the business organization. The authority for the system is Title 38, United States Code, chapter 73, section 7301.

Disclosure of PII, that if disclosed may expose the respondent/subject to financial loss or identity theft.
Disclosure of military service details that may compromise the individual's reputation, circumstances, or safety.

Disclosure of medical, personal, or other information that may compromise the individual's reputation, circumstances, or safety.

Disclosure of participation in a study or activity, where knowledge of participation may adversely impact the individual's reputation or circumstances.

Mitigation:
Information will be secured on the system through access controls, personnel security awareness and training, regular auditing of information and information management processes, careful monitoring of a properly authorized information system, control of changes to the system, appropriate handling and testing of contingencies and contingency planning, ensuring that all users of the information system are properly identified and authorized for access, and that they are aware of the rules and acknowledge that fact, by ensuring that any incident is handled expeditiously, properly maintaining the system and regulating the environment the system operates in, controlling media, evaluating risks and planning for information management and information system operations, by ensuring that the system and any exchange of information is protected, by maintaining the integrity of the system and the information stored in it, and by adhering to the requirements established in applicable contracts.

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.

Researchers seek this information for various investigative purposes.

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
First and Last Name	Further Research purposes/File Identification purposes	N/A
Personal Email Address	Further Research purposes/File Identification purposes	N/A
Date of Birth (DOB)	Further Research purposes/File Identification purposes	N/A
Home Address	Further Research purposes/File Identification purposes	N/A
Zip Code	Further Research purposes/File Identification purposes	N/A
Personal Telephone Number	Further Research purposes/File Identification purposes	N/A
Emergency Contact Number	Further Research purposes/File Identification purposes	N/A
Gender identity	Further Research purposes/File Identification purposes	N/A
Race and Ethnicity	Further Research purposes/File Identification purposes	N/A
Religion	Further Research purposes/File Identification purposes	N/A
Pronouns	Further Research purposes/File Identification purposes	N/A
Sexual orientation	Further Research purposes/File Identification purposes	N/A
Last 4 SSN and Full SSN	Further Research purposes/File Identification purposes	N/A
Preferred written language	Further Research purposes/File Identification purposes	N/A
Education Type	Further Research purposes/File Identification purposes	N/A
Age	Further Research purposes/File Identification purposes	N/A

Education Level	Further Research purposes/File Identification purposes	N/A
Branch of service	Further Research purposes/File Identification purposes	N/A
Time served	Further Research purposes/File Identification purposes	N/A
Active-duty status	Further Research purposes/File Identification purposes	N/A
Veterans PII: PII may be gathered such as coded pain scores, generic employment information, movement/activity/exercise data, satisfaction, and quality improvement data.	Further Research purposes/File Identification purposes	N/A
Blood pressure, sleep patterns, stress response, drug usage, participant experience with study.	Further Research purposes/File Identification purposes	N/A
A range of factors including (but not limited to) physical and mental health history, current functioning and symptoms, treatment satisfaction, and quality of life. All measures administered are IRB approved. (Pictures of subject weight on scale, only subject's feet will be visible).	Further Research purposes/File Identification purposes	N/A
Service-connected disability, and percentage	Further Research purposes/File Identification purposes	N/A
Medical information (to include Injury/Diagnosis)	Further Research purposes/File Identification purposes	N/A
Clinician Assessor-reported data (including interview data, and ratings of responses to our interventions).	Further Research purposes/File Identification purposes	N/A
Clinician Therapist-rated data (including ratings of responses in-session, and provider's views on acceptability, feasibility, tolerability, and utility of our assessment and intervention efforts).	Further Research purposes/File Identification purposes	N/A
Narrative information (experiences, recommendations, more detailed description)	Further Research purposes/File Identification purposes	N/A

Personal Knowledge of Program, Personal Barriers to program, Personal Values of Program	Further Research purposes/File Identification purposes	N/A
Patient-reported data such as pain scores, employment information, exercise data, height/weight, medications, patient satisfaction, suggestions for improvement, other clinical related questions intended to gauge patient satisfaction and improve performance. Surveys can also be constructed to obtain employee feedback on processes and procedures	Further Research purposes/File Identification purposes	N/A
Veteran payment preference	Further Research purposes/File Identification purposes	N/A
Media and technology usage	Further Research purposes/File Identification purposes	N/A

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?

Researchers/users may conduct analysis using in-product analysis tools. The analysis performed would vary project-to-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.

Research projects supported by Qualtrics may perform a variety of analyses of privacy-related data. Researchers may perform analysis using Excel and a Statistical Analysis System (SAS) or a host of other applications used for research purposes. New information about individuals may be generated as inputs to analysis or as intermediate products during

analysis. Privacy-related data are most often not included in the final, deliverable research results.

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?

The system is FedRAMP approved, and these measures are described in the FedRAMP documentation which can be found on the FedRAMP documentation repository, OMB MAX.

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).

The system is FedRAMP approved, and these measures are described in the FedRAMP documentation. Qualtrics offers a tool to enable customers to regulate the collection of personal data / personally identified information (PII). The tool can be configured to flag sensitive data requests (as defined by customer) and redact sensitive data from responses. See - https://www.qualtrics.com/support/survey-platform/sp-administration/data-privacy-tab/compliance-assist/ for details.

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

The system is FedRAMP approved, and these measures are described in the FedRAMP documentation. Information on accordance with OMB Memorandum M-06-15 would be included in that documentation.

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?

The system is FedRAMP approved, and these measures are described in the FedRAMP documentation. Qualtrics treats all data as highly confidential and promises to safeguard data as it would its own. As accounts are unmonitored and the End-User determines what Data to collect, Qualtrics cannot classify or represent the data. All data are processed equally regardless of their meaning or intent.

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?

The system is FedRAMP approved, and these measures are described in the FedRAMP documentation. Qualtrics offers a tool to enable customers to regulate the collection of personal data / personally identified information (PII). The tool can be configured to flag sensitive data requests (as defined by customer) and redact sensitive data from responses. See - https://www.qualtrics.com/support/survey-platform/sp-administration/data-privacy-tab/compliance-assist/ for details. Please refer to the Using the Service section of the Cloud Security and Privacy Framework. The Cloud Security Framework, along with various industry-standard security certifications, questionnaires, and more security artifacts can be requested here: https://www.qualtrics.com/trust-center/.

2.4c Does access require manager approval?

The system is FedRAMP approved, and these measures are described in the FedRAMP documentation. Access to Qualtrics is governed by the Qualtrics ORD project team who follows a detailed process for allowing system access.

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

All activities including access to all data inside each Qualtrics project instance is capable of being tracked using. robust audit capabilities inherent in the Qualtrics platform

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

The system is FedRAMP approved, and these measures are described in the FedRAMP documentation. The end users are responsible for assuring safeguards for the PII.

Section 3. Retention of Information

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

3.1 What information is retained?

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

All VA research information is retained by the Qualtrics system or exported from the system into VA approved repositories as required by records control schedule guidelines

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.

Records are scheduled in accordance with RCS 10–1, 8300.6, temporary disposition, cutoff at the end of the fiscal year after completion of the research project. Destroy six (6) years after cutoff. May retain longer if required by other Federal regulations or the European General Data Protection regulations. (DAA–0015–2015–0004, item 0032)

3.3 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.

Retention schedules are determined and approved at the project level. VHA Record Control Schedule 10-1 contains the record control schedule for research records. VA Facility research records are part of the 8300-schedule found in https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf. All research records, particularly FDA regulated, are not going to have the same retention period because if FDA requires that record to be kept past the standard retention period, which is 6 years, then the applicable federal requirement is going to apply.

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

Yes

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

Records are scheduled in accordance with RCS 10–1, 8300.6, temporary disposition, cutoff at the end of the fiscal year after completion of the research project. Destroy six (6) years after cutoff. May retain longer if required by other Federal regulations or the European General Data Protection regulations. (DAA–0015–2015–0004, item https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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

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

Sensitive information is disposed in accordance with VA policy and/or as directed by the contracting VA organization. Mechanisms available include shredding for paper and other materials, secure erasure for digital storage media, degaussing for magnetic media, and physical destruction for anything not securable by other means. Electronic data and files of any type, including PHI, SPI, Human Resources records, and more are destroyed in accordance with the Media Sanitization section of the VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and are compliant with NIST SP 800-88. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle Bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.https://www.va.gov/vapubs/search_action.cfm?dType=1

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.

Use of Qualtrics is dictated by principal investigators and study staff. When possible, researchers will minimize the use of PII and use alternative de-identified data.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System 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:
The privacy risk is that sensitive data will be kept longer than necessary and thus would be subject to risk for a longer period-of-time.

Mitigation:
Records are scheduled in accordance with RCS 10–1, 8300.6, temporary disposition; cutoff at the end of the fiscal year after completion of the research project. Destroy six (6) years after cutoff. May retain longer if required by other Federal regulations or the European General Data Protection regulations. (DAA–0015–2015–0004, item 0032)

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 <**Information System Name**> consists of <**number**> 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 <**Information System Name**> 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.)	**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**

that contains PII/PHI					
N/A					

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***
N/A	N/A	N/A	N/A

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: Qualtrics does not share, receive or transmit information to any internal organizations.

Mitigation: Qualtrics does not share, receive or transmit information to any internal organizations.

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.***	***List the method of transmission and the measures in place to secure data***

			that permit external sharing (can be more than one)	
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: Information is not shared outside of the Department.

Mitigation: Information is not shared outside of the Department.

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.

Notices are dependent on individual study protocols. System users will be instructed to provide Privacy Notice or the following SORN: Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA
34VA10 / 86 FR 33015
2021-13141.pdf "

6.1b If notice was not provided, explain why.

Notices are dependent on individual study protocols. System users will be instructed to provide Privacy Notice or the following SORN: Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA
34VA10 / 86 FR 33015
2021-13141.pdf "

.

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

Individuals are notified prior to data collection in accordance with VA policy and direction by VHA. "Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA
34VA10 / 86 FR 33015
2021-13141.pdf "

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.

Research activities that collect information from individuals are typically surveys in which participation by the individual is wholly voluntary. No penalties attach to refusal to participate, though incentives sometimes provided to encourage participation are not typically given to those who choose not to do so.

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.

Research activities that collect information from individuals are typically surveys in which analysis and reporting are the only uses. That is, participation is consent to sole intended use.

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:
Notice is not provided to the individual, or consent is not sought or is not adequately explained, prior to collection of information.

Mitigation:
Privacy-related information collected is commonly not included in final, deliverable research results.

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.***

Individuals seeking information regarding access to and contesting of records in this system related to research project submissions or participation in research projects may write, call or visit the VA location where the records were initially generated.

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)?

System is not exempt from Privacy Act.

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?

This platform falls under the research System of Records Notice (SORN) 34VA12 Research SORN Veteran, Patient, Employee, and Volunteer Research and Development Project Records—VA (34VA12). Individuals seeking information regarding access to and contesting of records in this system related to research project submissions or participation in research projects may write, call or visit the VA location where the records were initially generated.

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 contact the project-level individual named on the website or survey materials. This is dependent on the scientific protocol. For projects that allow changes in data that's already been provided, each subject will have to contact the Principal Investigator (PI) if they would like to amend information provided in a survey.

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 notified of these procedures in the survey materials, website, or privacy notice, and it is the responsibility of the PI to ensure individuals are informed of the procedures for correcting their information.

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

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

In addition to contacting project staff, survey respondents often have the option of supplementing, editing, or deleting their contact information and survey responses.

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:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

Principle of Individual Participation: 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.

Principle of Individual Participation: 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:

Privacy Risk: There is a risk that the subject accidentally provides incorrect information in their response to a Qualtrics questionnaire or survey which could misrepresent their knowledge and/or abilities.

Mitigation: Subjects provide information directly to the Qualtrics application. If needed, individuals may provide updated responses for their records by corresponding with the study's Principal Investigator or administrative staff.

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?

Individuals are sent links to access surveys via the internet.

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?

Users from outside agencies are not granted access to the 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.

Brand Administrators who are the Qualtrics system administrators in VA determine access levels and user types of survey participants. Brand Administrators have control over organizational and security settings within the brand.

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?

No

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

Yes

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

Certain Qualtrics staff have technical access to information as necessary which may include privacy sensitive responses provided by subjects. Qualtrics does not access individual accounts, or the data associated with client accounts unless specifically authorized for technical reasons. Qualtrics staff will only access VA Research account info and data as authorized by the VA project officer(s) or project director(s) of the project(s) to which everyone is assigned.

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 receive VA VA Privacy and Information Security Awareness and Rules of Behavior (WBT) and Privacy and HIPAA Training for Curriculum DVA-002.

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

8.4a If completed, provide:

1. *The Security Plan Status:* Compliant
2. *The System Security Plan Status Date:* 06/09/2023
3. *The Authorization Status:* Authority to Operate
4. *The Authorization Date:* May 10, 2024
5. *The Authorization Termination Date:* May 10, 2026
6. *The Risk Review Completion Date:* 06/09/2023
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.***

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)***

This system is a Software as a Service (SaaS) that uses cloud technology. The system is currently FedRAMP Authorized and active on the FedRAMP Marketplace under FedRAMP ID [F1606097904].

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. VA retains ownership of the data per the contract language.

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.

Under Section 3.5 of the General Terms and Conditions for Qualtrics Services, the customer grants Qualtrics the right to use certain ancillary data provided such data is anonymized and aggregated.

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.

Qualtrics is responsible as a data processor (not the data controller) for the privacy and security of data stored in the Qualtrics system. The specific obligations with respect to those subjects are outlined in Section 4 and Exhibit A of the General Terms and Conditions for Qualtrics Services.

Qualtrics FedRAMP Overview

- Qualtrics is FedRAMP authorized based on an annual assessment that is conducted by a Third Party Assessment (3PAO), with the outcomes being reports that are reviewed by Federal agencies. If the agency finds that our Security Assessment Report (SAR) and other applicable FedRAMP documents are acceptable, they will give us an Authority to Operate (ATO). The purpose of the FedRAMP program is to eliminate the need for agencies to do individual audits on cloud service providers and to allow agencies the ability to leverage standardized documentation across the work we've already done.

- Our FedRAMP Package outlines our compliance with hundreds of the rigorous NIST 800-53 security standards. These standards and controls are cross-referenced with such standards as ISO 27001/2, PCI, and HIPAA (Hitech Act). Security experts recognize FedRAMP as one of the highest non-military security programs.

FedRAMP Package Request

- Federal Government personnel can request Qualtrics' FedRAMP package through the FedRAMP Marketplace by completing the package request form: https://marketplace.fedramp.gov/products/F1606097904

- Qualtrics package ID is F1606097904

Other Security-related Resources

- **FedRAMP Marketplace:** https://marketplace.fedramp.gov/products/F1606097904
- **Security One-Pager:** https://www.qualtrics.com/security-statement/
- **Security Trust Center:** https://www.qualtrics.com/trust-center/
  Qualtrics homepage where clients can request information needed about our security, privacy, and compliance. Fill out the request to receive access to the security documents and certifications we make available.
- **Qualtrics VPATs:** https://www.qualtrics.com/commitment-to-accessibility/

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

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

N/A as the system does not use RPA.

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 provided in this Privacy Impact Assessment is true and accurate.

MICHELLE CHRISTIANO

Digitally signed by MICHELLE CHRISTIANO
Date: 2025.02.05 10:46:45 -05'00'

Privacy Officer, Michelle Christiano

ERICK DAVIS

Digitally signed by ERICK DAVIS
Date: 2025.02.06 10:58:26 -06'00'

Information Systems Security Officer, Erick Davis

HENNA GROVER

Digitally signed by HENNA GROVER
Date: 2025.02.06 16:16:33 -05'00'

Information Systems Owner, Henna Grover

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).

Privacy Act System of Records 34VA10 :
https://www.federalregister.gov/documents/2010/05/27/2010-12758/privacy-act-of-1974-system-of-records

HELPFUL LINKS:

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

General Records Schedule 1.1 Financial Management and Reporting Records (FSC)
https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

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

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

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

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