Privacy Impact Assessment for the VA IT System called:

Surgery Risk Assessment Database

Veterans Health Administration (VHA)
National Surgery Office (NSO)

Date PIA submitted for review:

07/25/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.katz-johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Alomar-Loubriel, Richard	Richard.Alomar-Loubriel@va.gov	787-641-7582
Information System Owner	Sines, Tony	Tony.Sines@va.gov	316-249-8510

Abstract

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

The Surgery Risk Assessment Database and the associated processes are designed to document, collect, organize, and transmit surgery case data. It collects non-cardiac assessment data from all the VA Medical Centers in order to process and store them in a database file at the Austin Information Technology Center (AITC). Due to lower volume (about 5,000 cases annually verses 400,000 for non-cardiac), the Cardiac risk assessments are sent via a separate data stream directly to the VA National Surgery Office in Denver, CO via Veterans Health Information Systems and Technology Architecture's (VistA) MailMan messages. (MailMan is software for managing electronic mail and can run processes to route electronic mail.)

Overview

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

1 *General Description*

A. *The IT system name and the name of the program office that owns the IT system.*

System Name: Surgery Risk Assessment Database (SRA). Program office: National Surgery Office (NSO)

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

The SRA is part of the VA Surgical Quality Improvement Program (VASQIP). This database contains assessments of selected surgical operations performed at Veteran Affairs Medical Centers (VAMCs). SRA requires that the surgery is Major (as defined by the Current Procedural Terminology (CPT) codes assigned to the surgery), it must not be cardiac related, and it may not be concurrent with another surgery. Frequently performed other types of surgeries may also be excluded. Nurse reviewers at VAMCs gather the information from surgical data located in the Veterans Health Information Systems and Technology Architecture (VistA) environment. Information is also collected from pre- and post-operative charts and from interviews with patients. This information is entered into VistA and transmitted daily by a batch process to the database located at AITC. While the database has been in operation since 1995, the system only contains data for the previous two fiscal years. The data from previous fiscal years is archived if later retrieval is needed. Valid transmissions are sent to the VASQIP office at Denver for analysis. Information from non-assessed surgeries is transmitted from the VAMCs to the database at AITC monthly. This is also passed along to VASQIP at Denver. The users of this database include the VASQIP Executive Board.

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

VA Owned and VA Operated

2. *Information Collection and Sharing*

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

Currently housing approximately 812,000 unique records, tied to an unknown number of individual persons.

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

This database contains assessments of selected surgical operations performed at Veteran Affairs Medical Centers (VAMCs). Information is also collected from pre-and post-operative charts and from interviews with patients.

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

SRA shares information with VistA and the NSO.

G. *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*

System is operated on AITC only.

3. Legal Authority and SORN

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

79VA10 - Veterans Health Information Systems and Technology Architecture (VistA) Records VA; https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

No amendment required.

D. System Changes

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

No. PIA is being resubmitted as a result of a system OS upgrade from RHEL 7 to RHEL 8 and IRIS 2020 to IRIS 2022.

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

No

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☐ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information

☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers*
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☒ Gender

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

Age, Surgical Case Information, Procedure Code(s), DX code(s), Surgical Quality Nurse Name (person whom completed Surgical Assessment)

PII Mapping of Components (Servers/Database)

Surgery Risk Assessment Database consists of one key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Surgery Risk Assessment Database and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VistA (All VAMC VistA systems)	Yes	Yes	Name, SSN, DoB, Age, Personal Mailing Address, Personal Phone Number(s), Race/Ethnicity, Gender, Surgical Procedure, Procedure Code(s), DX code(s), Surgical Quality Nurse Name	Required per system integration	See VistA PIA

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

VAMC surgical staff collect the information from the patient and the patients' medical record. Information is then sent to the SRA where it is stored. The National Surgery Office will query the database for reports.

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.*

N/A.

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

N/A.

1.3 How is the information collected?

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

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

Information is collected from the Patient by the VAMC staff. SRA personnel do not collect any information.

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

N/A.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

The data is maintained and validated at each VAMC by the surgical nurse coordinator at the site where it is collected. SRA is only a repository, so the data is transmitted via messaging and VistA will receive a confirmation message if an upload is successful. If there are errors, the site is notified and it would be either corrected or a Service Now (SNOW) ticket would be created for assistance. The system is monitored daily by OIT technical staff assigned to support the Surgery Risk Assessment Database. The OIT technical staff evaluate the number of transmission messages received from VA Medical Centers and identify whether any transmission errors or software errors occurred after checking the error trap.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

N/A.

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

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

Information is collected under 79VA10 - Veterans Health Information Systems and Technology Architecture (VistA) Records VA. AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, section 7301(a).

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

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

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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: The system receives and retains PII and PHI on Veterans. If this information were breached or accidentally disclosed to inappropriate parties or the public, it could result in personal and financial harm to the individuals impacted and have an adverse negative effect to VA.

Mitigation: Data received and retained will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.

Section 2. Uses of the Information

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

2.1 Describe how the information in the system 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.

Data documented in the Risk Assessment Database is validated, formatted, analyzed, and developed into reports by the NSO using the VA Surgical Quality Improvement Program (VASQIP) system in a secure online environment.

- Name used to identify patient.
- Race used to identify patient and for statical analysis.
- SSN used to identify patient.
- DOB used to identify patient.
- Age used to identify patient and statical analysis.
- Gender used for statical analysis.
- Address and Phone used to identify patient.
- Surgical Case info used for statical analysis.
- Procedure codes used for statical analysis.
- DX codes used for statical analysis.
- Surgical Quality Nurse used for statical analysis

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

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

Once the server has successfully parsed the non-cardiac VistA MailMan message, file validation messages are sent to the Surgical Quality Nurse (SQN), stating that assessment has been successfully processed and to the local VistA Surgery Package, updating the assessment's status from "complete" to "transmitted." After the Risk Assessment Download file, Surgical Case Workload Totals, and Workload Incomplete Assessments text files have been created, a message is sent to members of the SRA DOWNLOAD mail group. The files are encrypted and sent to the NSO staff via Surgery Risk Assessment Monthly Download Outlook Distribution Group.

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.

Information is only maintained by the SRA; queries and/or reports would be done so by the NSO (external to the SRA, though internal to the VA).

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

Data at rest is protected by FIPS compliant file encryption. Cryptographic Key management servers host the key, if access is lost to the key management server, the database is locked. Security keys have various uses in the Surgery Risk Assessment package and must be assigned as needed before using the package.

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

SRA only displays the last 4 of the SSN, but the database retains the entire social security number.

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

Access to SRA is limited and entire database is encrypted.

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

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

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

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 OIT staff supporting the SRA must have full access to all aspects of the system. This includes programmer level access to troubleshoot and sustain the product. This level of access is given only to a small number of staff specifically assigned and privileged to fulfill this role

NSO staff will have access to print risk assessment download, display VISN/Medical Center Alignment, List of VISNS and Surgical Nurse Contacts, download monthly workload reports and create surgery risk assessment downloads

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

Criteria, procedures, controls, and responsibilities are documented within the SRA Access Control and Privacy Standard Operating Procedures (SOPs).

2.4c Does access require manager approval?

Yes

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

VistA auditing is enabled on SRA.

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

The ISO, ISSO, System Administrator(s), and Privacy Officer

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*

As part of the nightly tasked option Check for Risk Assessment Transmission Errors (SRAFERR), the software checks to determine whether it is time to purge old assessments. If the date is December 31st, the software will delete all entries in the SURGERY RISK ASSESSMENT file prior to the previous two fiscal years. For example, when run on December 31, 2022, all entries with a date prior to October 1, 2020 will be deleted.

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

As part of the nightly tasked option Check for Risk Assessment Transmission Errors (SRAFERR), the software checks to determine whether it is time to purge old assessments. If the date is December 31st, the software will delete all entries in the SURGERY RISK ASSESSMENT file (139) prior to the previous two fiscal years. For example, when run on December 31, 2022, all entries with a date prior to October 1, 2020 will be deleted.

The current data retention length is less than the approved length per the retention scheduled approved by the National Archives and Records Administration (NARA). As of July 2023, The SRA is currently investigating a patch to the system to bring it fully in line with the requirement to maintain all data for 3 years prior to deletion. This efforts to implementing this change will be tracking within the VA's GRC tool under privacy control DM-2. Of note, all records that go through SRA are maintained separately within the originating system and then at the NSO.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

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

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

Yes.

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

SRA follows the VistA records retention schedule:

RCS 10–1, Item 2000.2 Information Technology Operations and Maintenance Records destroy 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use (DAA–GRS–2013–0005– 0004, item 020). RCS10–1, Item 2100.3 2100.3, System Access Records destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use (DAA–GRS–2013–0006– 0004, item 31). rcs10-1.pdf (va.gov)

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.

Elimination of electronic data is inherited from the AITC. All hardware is housed in AITC where the SRA application and databases reside. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=742&FType=2 Version Date: January 2, 2019 Page 13 of 26 Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008), http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=416&FType=2. When required, this data is deleted from the file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1. Additionally, this system follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

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.

SRA information will not be used for testing new applications or information systems prior to deployment.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

Privacy Risk: Privacy risk is unauthorized persons may access the SRA.

Mitigation: Privacy risk is mitigated because access to the information is limited by permissions and access controls and only essential elements needed to report and record operations are retained. SRA also uses encryption for data stored in the system.

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?

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
National Surgery Office (NSO)	SRA is part of the VASQIP with the NSO. Supports assessments of surgical operations performed at VAMCs	Name, SSN, DoB, Age, Personal Mailing Address, Personal Phone Number(s), Race/Ethnicity, Gender, Surgical Procedure, Procedure Code(s), DX code(s), Surgical Quality Nurse Name	SMTP Mail message Outlook NSO DL. Text file is encrypted, and password protected

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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

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

Follow the format below:

Privacy Risk: Unauthorized persons accessing database and viewing patient information

Mitigation: The privacy risk to the SRA information is minimized through various layers of security boundaries. The SRA database resides in the secured AITC which has FIPS 140-2 encryption enabled. AITC practices continuous monitoring through various tools and the overall environment is monitored by CSOC.

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.

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

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

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

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

Data Shared with External Organizations

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

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

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

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:

<u>Privacy Risk:</u> N/A systems does not share information with external organizations.

<u>Mitigation:</u> N/A systems does not share information with external organizations.

Section 6. Notice

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

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

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

In Accordance with SORN 79VA10 which was published in the federal register 12/23/20 explains the authority, purpose, categories of information, routine uses and record access procedures. All individuals who receive care at VHA are provided with the Notice of Privacy Practices.

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

N/A.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

In Accordance with 79VA10 - Veterans Health Information Systems and Technology Architecture (VistA) Records VA which was published in the federal register 12/23/20 explains the authority, purpose, categories of information, routine uses and record access procedures. All individuals who receive care at VHA are provided with the Notice of Privacy Practices.

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.

Information is collected under 79VA10 - Veterans Health Information Systems and Technology Architecture (VistA) Records VA. Without providing the needed information, SRA may not provide intended results for patient care.

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.

Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without consent and when they will be asked to provide consent. Information is used, accessed, and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

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

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

<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:

<u>Privacy Risk:</u> There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.

<u>Mitigation:</u> This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records, The NOPP is also available at all VHA medical centers from the facility Privacy Officer.
The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

Section 7. Access, Redress, and Correction

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

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

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may *also include additional access provisions****. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

The contact information for each medical center is listed in the System of Record Notice 79VA10. Additionally, the Privacy Officers monitor that staff are aware of record access and amendment processes so any staff member can direct an individual to Health Information Management or the facility Privacy Officer.

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).

N/A.

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.

N/A.

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.

Contact information is listed in the System of Record Notice 79VA10. Individuals complete a written request for an amendment that is processed in accordance with VHA Directive 1605.01. Additionally, the Privacy Officers monitor that staff are aware of record access and amendment processes so any staff member can direct an individual to Health Information Management or the facility Privacy Officer.

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.*

Contact information is listed in the System of Record Notice 79VA10. Additionally, the Privacy Officers monitor that staff are aware of record access and amendment processes so any staff member can direct an individual to Health Information Management or the facility Privacy Officer.

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.

N/A.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: Individuals may be unaware of the process for access, redress, and correction.

Mitigation: VHA Privacy Officers conduct quarterly monitoring and ongoing education to ensure that VHA staff are aware of the processes in an effort to assist and direct individuals.

Section 8. Technical Access and Security

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

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

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

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

All personnel that have access to the SRA are VA employees. Access is granted though a captive account called FOUVISTA. Once the user accesses the database, they are required to enter an access and verify code. Access and verify codes are provide after approved application in FOURWARD administrators. Alternatively, users may login to VistA through PIV.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

N/A.

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.

There are Privileged User Accounts and Standard User Accounts.

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.

N/A all SRA staff are VA employees.

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.

There is no additional security training for SRA personnel over and above training required by VA.

All employees are required to complete VA Privacy and Information Security Awareness Training and Rules of Behavior on an annual basis. Employees that have access to PHI are also required to take Privacy and HIPAA focused training on an annual basis.

Annual training for the National Rules of Behavior is performed through the Talent Management System (TMS).

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved.
2. *The System Security Plan Status Date:* 10-Feb-2023
3. *The Authorization Status:* Authorized to Operate
4. *The Authorization Date:* 24-Apr-2023
5. *The Authorization Termination Date:* 21-Oct-2023
6. *The Risk Review Completion Date:* 21-Apr-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 No or In Process, provide your ***Initial Operating Capability (IOC) date.***

N/A.

Section 9 – Technology Usage

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

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service

(MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

N/A.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

N/A.

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.

N/A.

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.

N/A.

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.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2023.08.01 09:57:49 -04'00'

Privacy Officer, Nancy Katz-Johnson

RICHARD ALOMAR-LOUBRIEL 139039

Digitally signed by RICHARD ALOMAR-LOUBRIEL 139039
Date: 2023.08.03 11:39:42 -04'00'

Information System Security Officer, Alomar-Loubriel, Richard

Tony L. Sines 167047

Digitally signed by Tony L. Sines 167047
Date: 2023.08.03 14:13:58 -05'00'

Information System Owner, Tony Sines

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).

79VA10 - Veterans Health Information Systems and Technology Architecture (VistA) Records VA; https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

HELPFUL LINKS:

Record Control Schedules:

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

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

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

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices