Privacy Impact Assessment for the VA IT System called:

Records Retrieval System (RRS)

VA Central Office (VACO)

(FSC) Financial Services Center, (FTC) Financial Technology Center PMO

eMASS ID #123

Date PIA submitted for review:

02/26/2024

System Contacts:

System Contacts

Title	Name	E-mail	Phone Number	Signature Required
Privacy Officer	*Pamela M. Smith*	*Pamela.Smith6@va.gov*	*512-386-2246*	*Yes*
Information System Security Officer	*Ronald Murray*	*Ronald.Murray2@va.gov*	*(512) 460-5081*	*Yes*
Information System Owner	*Jonathan Lindow*	*Jonathan.Lindow@va.gov*	*737-802-9565*	*Yes*

Abstract

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

Records Retrieval System (RRS) is a VA-intranet application to facilitate submittal and retrieval of retired records in support of Records Center and Vault (RCV) physical record storage and recall processes. RRS provides a user interface to complete, save, and print record submittal and request forms (VA Forms 0244 and 0245). The VA Form 0244 is used to request the storage of records from the owning VA facility to the RCV warehouse. The VA Form 0245 is used by the records-owning facility to request a recall of retired records stored at RCV facilities. NOTE: For all answers, "File" and "Record" are used interchangeably.

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. What is the IT system name and the name of the program office that owns the IT system?

Records Retrieval System (RRS)
(FSC) Financial Services Center, (FTC) Financial Technology Center PMO

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

VA facilities use the RRS to complete and submit the VA Form 0244 electronically and print a hard copy to send with boxes of records transferred to the RCV for storage. The VA Form 0244 shows the RCV accession number of the shipment, the quantity and type of records being shipped for storage and when the boxes are eligible for destruction.

VA facilities also use the RRS to complete and submit the VA Form 0245 to recall hard copies of files from inside their stored boxes located at the RCV. The RCV ships the requested hardcopies to the owning facility and places a printed copy of the associated VA Form 0245 inside the box in place of the recalled file(s).

The RRS has a limited interface with the Records Management System (RMS), called Total Recall. The RMS database contains accession numbers, box numbers, locations, et al. within the RCV storage infrastructure. When a RCV records custodian clicks the

button to print a customer-submitted VA Form 0245, the RRS validates the accession number and box location against the RMS database. The RMS database does not process or contain PII.
Accession numbers, box numbers, box locations, and individual files are the key data fields that help locate the requested files via the VA Form 0245 records request. To locate individual files, the VA Form 0245 contains a "File Title:" field, which is commonly populated with the Veteran's Name. Also included on the form is a "File Number:" field, which is commonly populated with a Veteran's SSN, but is sometimes a VA Claim Number. The records owner determines how they catalog, index, and recalls their boxes of records.

If RCV Records Custodians are unable to locate a requested file in a specified box, they will send back a reference to the first and last files found in the box using the "Record Range:" field to assist the owning facility with verifying their internal records. When this happens, the "Record Range:" field resembles something like this: "Abraham, David 111223333 – Baskins, Bobby 333221111." None of the fields on the VA Form 0245 are labeled as Name and SSN, but the Veteran's Name and SSN are used on the VA Form 0245 to file and locate records, as per agency procedures.

C. Who is the owner or control of the IT system or project?
RRS is a web-based VA Owned and VA Operated application.

2. Information Collection and Sharing

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

The RCV averages 300 requests per day. Multiplied by 260 workdays per year times 6.25 years, approximately 500,000 records are retained for billing purposes. Older information is purged in accordance with applicable agency and/or NARA general records schedules.

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

The RRS has a limited interface with the Records Management System (RMS), called Total Recall. The RMS database contains accession numbers, box numbers, locations, et al. within the RCV storage infrastructure. When a RCV records custodian clicks the button to print a customer-submitted VA Form 0245, the RRS validates the accession number and box location against the RMS database. The RMS database processes limited PII for managing the request and folder locations. It does not share the PII with other databases internal or external. Accession numbers, box numbers, box locations, and individual files are the key data fields that help locate the requested files via the VA Form 0245 records request. To locate individual files, the VA Form 0245 contains a "File Title:" field, which is commonly populated with the Veteran's Name. Also included on the form is a "File Number:" field, which is commonly populated with a Veteran's SSN, but is sometimes a VA Claim Number. The records owner determines how they catalog, index, and recalls their boxes of records.

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

No information is shared with other systems.

G. Is 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?

Within the FSC logical boundary, RRS is hosted at Austin Information Technology Center (AITC) and the backup location Pittsburg Information Technology Center (PITC).

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

The legal authority to operate the IT system is Public Law 109-114 and Title 38, United States Code Chapter 5 Section 501(a) and Chapter 57. (https://www.oprm.va.gov/privacy/systems_of_records.aspx).
"Patient Medical Records VA", 24VA10A7 dated 10/02/2020. The SORN can be found online at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pd

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?

This system is not in the process of being modified.

4. System Changes

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

NO

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

Other PII/PHI data elements:

- File Name
- File Number
- File Title

PII Mapping of Components (Servers/Database)

Records Retrieval System consists of 7 key components (3 database, 4 webservers). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Records Retrieval System and the reasons for the collection of the PII are in the table below.

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

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
RRS Database Server aka "Vault Schedule"	Yes	Yes	PII - Name, SSN	Fill out a records request form (VA Form 0245), which require "File Name" and "File Number" (Veteran's Name and SSN) to locate hard copy of the records within the RCV warehouse.	RRS is an isolated application within the FSC. RRS is only used to request storage or retrieval of records from the RCV by VA employees. The SSNs are encrypted by the database. Data is encrypted at rest and in transit.
RMS Database Server 1	Yes	Yes	PII - Name, SSN	Fill out a records request form (VA Form 0245), which require "File Name" and "File Number" (Veteran's Name and SSN) to locate hard copy of the records within the RCV warehouse.	Misuse is minimal due to the limited functionality of RRS. RRS is only used to request storage or retrieval of records from the RCV by VA employees.

					The SSNs are encrypted by the database. Data is encrypted at rest and in transit.
RMS Database Server 2	Yes	Yes	PII - Name, SSN	Fill out a records request form (VA Form 0245), which require “File Name” and “File Number” (Veteran’s Name and SSN) to locate hard copy of the records within the RCV warehouse.	Misuse is minimal due to the limited functionality of RRS. RRS is only used to request storage or retrieval of records from the RCV by VA employees. The SSNs are encrypted by the database. Data is encrypted at rest and in transit.
RRS Web Server 1	Yes	Yes	PII - Name, SSN	Fill out a records request form (VA Form 0245), which require “File Name” and “File Number” (Veteran’s Name and SSN) to locate hard copy of the records within the RCV warehouse.	Misuse is minimal due to the limited functionality of RRS. RRS is only used to request storage or retrieval of records from the RCV by VA employees. The SSNs are

					encrypted by the database. Data is encrypted at rest and in transit.
RRS Web Server 2	Yes	Yes	PII - Name, SSN	Fill out a records request form (VA Form 0245), which require “File Name” and “File Number” (Veteran’s Name and SSN) to locate hard copy of the records within the RCV warehouse.	Misuse is minimal due to the limited functionality of RRS. RRS is only used to request storage or retrieval of records from the RCV by VA employees. The SSNs are encrypted by the database. Data is encrypted at rest and in transit.
RRS Web Server 3	Yes	Yes	PII - Name, SSN	Fill out a records request form (VA Form 0245), which require “File Name” and “File Number” (Veteran’s Name and SSN) to locate hard copy of the records within the RCV warehouse.	Misuse is minimal due to the limited functionality of RRS. RRS is only used to request storage or retrieval of records from the RCV by VA employees. The SSNs are encrypted by the

					database. Data is encrypted at rest and in transit.
RRS Web Server 4	Yes	Yes	PII - Name, SSN	Fill out a records request form (VA Form 0245), which require “File Name” and “File Number” (Veteran’s Name and SSN) to locate hard copy of the records within the RCV warehouse.	Misuse is minimal due to the limited functionality of RRS. RRS is only used to request storage or retrieval of records from the RCV by VA employees. The SSNs are encrypted by the database. Data is encrypted at rest and in transit.

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?

VA representatives working at VA facilities are the source of the “File Title” and “File Number”.

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.

Information from sources other than the individual is not required.

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

When the owning VA facility requests a Veteran's record, they are required to provide file references (Veteran's Name and SSN) as part of the request form so RCV representatives know which file(s) to pull from their box. Veteran information labeled as an individual's Name and/or SSN is not used or stored within the RRS.

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?

VA employees with access to the RRS portal, fill out a records request form (VA Form 0245), which require "File Name" and "File Number" (Veteran's Name and SSN) to locate hard copy of the records within the RCV warehouse.

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?

The form is not part of the Paperwork Reduction Act.

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.

Veteran physical records stored within accession numbered boxes are referenced by "File Name" and "File Number" (Veteran Name and SSN), so when a VA facility requests one of their Veteran's records from the RCV using the RRS to generate a VA Form 0245, the requesting VA facility's representative must provide these fields as reference to locate the requested hardcopy record within the box.

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?

The system does not check for accuracy by accessing a commercial aggregator of information\.

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

Citation to the legal authority as identified in the based on the SORN listed in this document. See below:

24VA10A7 / 85 FR 62406

Title 38, United States Code, Sections 501(b) and 304.

2020-21426.pdf (govinfo.gov) .

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Privacy Risk: Sensitive Personal Information including personal contact information, service information and benefit information may be released to unauthorized individuals.

Mitigation: AITC adheres to information security requirements instituted by the VA Office of Information Technology (OIT).

•All employees with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
•The MS-Outlook setting to encrypt email messages containing PII/PHI/SPI is required of all users.

Section 2. Uses of the Information

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

2.1 Describe how the information in the system that will be used in support of the program's business purpose.

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

PII/PHI Data Element	Internal Use	External Use
<<Name>>	File Identification purposes	Not used

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?

RCV does not make determinations nor collect/analyze data in support of determinations.

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.

RCV does not make determinations nor collect/analyze data in support of determinations.

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?
The SSNs are encrypted by the database. Data is encrypted at rest and in transit.

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

The user's access can be limited by agency and station number. Users that work on the RRS system are the ones that access the Veteran's full SSN.

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

Per the Storage Administrator, all SAN storage at data centers is encrypted. Therefore, as all servers for the system are virtual and reside on the SAN storage, all information at rest is encrypted.

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?

Potential for misuse is minimal due to the limited functionality of RRS. RRS is only used to request storage or retrieval of records from the RCV by VA employees but does not collect information. Only the individuals that are registered in Active Directory that has access to RRS but also required to follow Health Insurance Portability and Accountability Act HIPAA, Health and Human Services HHS, Office of Health Informatics OCR and Veterans Health Administration VHA guidelines or agreements with signature before accessing VA internal infrastructure of the VA (Including Veteran records). In Version Date: October 1, 2021, Page 13 of 31 according to their permission, title, and duties from the Information Security Officer (ISO). All VA employees with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness & Rules of Behavior training annually.

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

Access procedures documented within the RRS User Guide.

2.4c Does access require manager approval?

Second, follow-up the profile request by sending a completed VA 9957 e-signed by the requester and their supervisor to the rcv.operations@va.gov email group who will open a YOURIT help desk ticket to activate the login. A guide that gives additional information about the login process and how to complete the VA 9957 is available by clicking the "Registration Instructions" link located below the RRS login button.

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

All RRS servers are monitored by the VA's Monitor Service Registry (MSR). Servers has monitoring and health check services configured utilizing the FSC Monitoring Services.

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

Safeguards are handled by VA's OIT.

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*

VA Form 0245 form data, to include "File Name" and "File Number" are stored within the RRS database. Hardcopies of the VA Form 0245 are stored within the boxes of the RCV warehouse.

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.*

The printed VA Forms 0244 and 0245 are the official agency records. The data remaining in the SQL table is used to justify RCV's monthly customer billing and is stored for 6 years and 3 months from the time submitted if no further necessity to freeze records beyond their scheduled retention dates. Some records are stored indefinitely to support litigation or other exempt purpose.

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

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

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

The VA 0244 and VA 0245 forms printed from the RRS serve as the official record for the agency. The only use for the remaining data in the SQL table verifies customer monthly billing charges and is retained until the billing documents are purged.
RCV customers adhere to VA records control schedules, such as VHA RCS 10-1 and VBA RCS VB-1 rcs10-1.pdf (va.gov)

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

Disposition Authority: Item: 010; DAA-GRS 2013-0003 0001

All guidance is located at https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

RRS retains all records indefinitely as per directions from RCV Records Center Vault Business Unit. (Business Unit POC – Kim Tuggle.)

VA/VHA provides the data in RRS to retire records to offsite storage, and to retrieve records from storage when agency need arises. The forms generated with the data are the Records Transmittal and Receipt, and Reference Request. This information is covered in RCS 006-1, GRS 4.1/020, Records Management Program records.

Item: 010; DAA-GRS 2013-0003 0001

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.

RRS adheres to NIST SP 800-88 Guidelines for Media Sanitization standards for record destruction, refer to NIST SP 800-88 Guidelines for Media Sanitization for a media destruction flowchart giving the details of the process.

Electronic records are retained as long as required (GRS Schedule 1.1, Item #10), and are destroyed IAW (In Accordance With) NARA disposition instructions. grs1-1.pdf (archives.gov)

At the Records Center Vault physical paper file are not scanned and digitized and indexed for archival purposes. The records are paper.

Paper records are shredded onsite in accordance with the retention control schedule. The RCV's RMS application tracks expiration dates and when notice of eligibility to destroy is sent to customer. The customer prints and signs the destruction authorization prior to execution.

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.

The RRS system does not use PII/PHI/SPI or production data for any testing or development purposes.

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: There is a risk that the information contained in the supporting RRS database tables will be retained for longer than necessary to fulfill the VA mission.

Mitigation: There is no public access and limited authenticated access to RRS database tables. VA facilities can check processing status of their requests by querying the associated SQL data table.

RCV adheres to the National Archives and Records Administration (NARA) retention control schedule. The RCV maintains a copy of the electronic requests for 6 years and 3 months to justify performance metrics and monthly customer billing charges.

RCV conducts hardcopy destruction via an onsite high security disintegrator. Electronic media is sent back to VA station owner for destruction.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
No internal sharing.	No internal sharing.	No internal sharing.	No internal sharing.
No internal sharing.	No internal sharing.	No internal sharing.	No internal sharing.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: No internal sharing.

Mitigation: No internal sharing.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, 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
N/A	N/A	N/A	N/A	N/A

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>
Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

Follow the format below:

Privacy Risk: No internal sharing. .

Mitigation: No internal sharing.

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.

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways:

- The System of Records Notice (SORN) "Patient Medical Records VA", 24VA10A7 dated 10/02/2020. The SORN can be found online at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

- This Privacy Impact Assessment (PIA) also serves as notice of the AITC Insurance Payment System. As required by the eGovernment Act of 2002, Pub. L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

RRS does not collect information. RRS does not require System of Records Notice.

However, if an individual wishes to remove consent for a particular use of their information, they should contact the nearest VA regional office or VHA facility, a list of which can be found at https://benefits.va.gov/benefits/offices.asp or https://www.va.gov/directory/guide/division_flsh.asp?dnum=1.

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

RRS does not collect information. Due to this the RCV is not required to provide notice.

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

The information for a records request is performed at the local level closest to the veteran. The notice information in 6.1b is the general information provided.

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.

VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)). RRS does not collect information. RRS does not require System of Records Notice. However, if an individual wishes to remove consent for a particular use of their information, they should contact the nearest VA regional office or VHA facility, a list of which can be found at - https://benefits.va.gov/benefits/offices.asp or https://www.va.gov/directory/guide/division_flsh.asp?dnum=1.

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.

VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually identifiable health information to carry out treatment, payment, or health care operations. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. RRS does not collect information. RRS does not require System of Records Notice. However, if an individual wishes to remove consent for a particular use of their information, they should contact the nearest VA regional office or VHA facility, a list of which can be found at https://benefits.va.gov/benefits/offices.asp or https://www.va.gov/directory/guide/division_flsh.asp?dnum=1.

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 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 Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: Privacy information may be collected prior to providing written notice.

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Impact Assessment and the Version System of Record Notice. This PIA serves as an informative resource for individuals to better understand what specific information is being processed through RRS.

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.***

RRS is used by VA entities to interface with the RCV. The VA Facility's RRS user can either request to store or retrieve paper records. RCV returns recalled hardcopies to the requesting VHA/VBA stations only. Individuals seeking access to their VA records may call (Toll Free 1-800-827-1000), write, or visit the nearest VA regional office or VHA facility. A list of l offices is available at http://benefits.va.gov/benefits/offices.asp orhttp://www.va.gov/directory/guide/division_flsh.asp?dnum=1 or direct to http://www.archives.gov/veterans/military-service-records/evetrecs-help.html

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)?

The system is not exempt from the access provisions of the 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?

The system is not a Privacy Act system.

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.

RRS is used by registered VA employees to store or recall paper records from the RCV. Public entities would contact their supporting VA facility, and the facility will follow the procedures outlined in VA Handbook 6300.4, Section 3. Procedures for Handling Requests for Access to Amendment of Records.

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.

RRS is used by registered VA employees to store or recall paper records from the RCV. RCV personnel do not provide any notifications or make any contact with the public. Individuals would contact their supporting VA regional office or VHA center to inquire about procedures for correcting his or her 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.

There is no formal redress for records stored with the RCV; however, Veterans and other beneficiaries may contact their supporting VA regional office or VHA center to learn how to access, correct, or contest their information.

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: Members of the public may not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: RCV personnel do not directly serve or interface with the public. Only authorized VA employees with valid network credentials can request access the RRS. RCV customers (Regional VA Centers, VA Hospitals, etc.) ensure Veterans are aware of how to access, correct, or contest their information.

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?

To request access to RRS, the users, which are internal VA employees and contractors, working at VA facilities, must have their supervisor submit an online form (VA Form 9957) as an NSD Request Ticket. Requestor's name and email address is confirmed against VA Active Directory when they initiate the online form. Requestors must provide Supervisor's Name and contact info, Records Custodian contact info, and requestor's contact info. After the requestor's Supervisor digitally signs the VA Form 9957 and submits to the NSD, RCV personnel must approve the request ticket prior to adding the requestor to the RRS access list.

Version Date: October 1, 2021Page 24 of 31RRS users can only create, edit, submit, and print either the VA Form 0244 or VA Form 0245.Authorized RCV employees with elevated privileges can mark records for deletion, add approved accounts, and view reports.

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?

- Access is restricted to VA employees in release of information and records management positions by agency and VA station id. Other government agencies do not have access to the system or the data. Information is not shared.

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 3 access levels: 1. Super User – VA IT Staff have ability to make all changes to system, software, and data contained within software. 2. Admin User – VA FSC staff that fill individual station requests made to store and retrieve records from the RCV warehouse. Admin User can manipulate (read, modify, delete) the storage and retrieval request data entered by the individual VA stations. 3. User – VA station users at regional offices and VA medical centers can create, submit, and view requests input into the system for their respective stations.

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.

To access RRS, all VA personnel (including VA civilians and contactors) that has access to RRS are required to follow HIPAA, HHS, OCR and all requirements under VHA guidelines and agreements with signature before accessing to VA internal infrastructure of the VA (Including Veteran records). In according to their permission, title and duties from the Information Security Officer (ISO). VA contractors must already have VA intranet access, and the required National Agency Check with Inquires (NACI) background investigation. A contractor's VA Supervisor must digitally sign a VA Form 9957 and submit to the National Service Desk (NSD). Authorized personnel at RCV have visibility to those request tickets, check their credentials against AD and if all checks out, grant access to RRS, which is documented via the NSD ticket. Contracts are reviewed quarterly by the COR. RCV contractors do not telework, so contractor access to RRS is controlled from the VA facility. When contractors leave their position, their accounts are marked for deletion by the COR.

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.

- No additional privacy training is required for access to RRS. RRS can only be accessed by VA intranet users. VA users are required to complete annual Privacy and Information Security Awareness & Rules of Behavior training, which is available in via the Talent Management System (TMS) course number VA 10176.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Current (Current as of March 25, 2024)
2. *The System Security Plan Status Date: Feb 9*, 2024
3. *The Authorization Status:* Full
4. *The Authorization Date:* Oct 19, 2023
5. *The Authorization Termination Date:* April 13, 2024
6. *The Risk Review Completion Date:* OCT 13, 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* HIGH

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 provided in this Privacy Impact Assessment is true and accurate.

PAMELA SMITH

Digitally signed by PAMELA SMITH
Date: 2024.04.01 16:28:11 -05'00'

Privacy Officer, Pamela M. Smith

RONALD MURRAY

Digitally signed by RONALD MURRAY
Date: 2024.04.02 09:18:44 -05'00'

Information Systems Security Officer, Ronald Murray

JONATHAN LINDOW

Digitally signed by JONATHAN LINDOW
Date: 2024.04.02 14:01:36 -05'00'

Information Systems Owner, Jonathan Lindow

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).

- The System of Records Notice (SORN) "Patient Medical Records VA", 24VA10A7 dated 10/02/2020. The SORN can be found online at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

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

VA Publications:
https://www.va.gov/vapubs/

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

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