Privacy Impact Assessment for the VA IT System called:

Applications for Visit Summaries

Veterans' Health Administration (VHA)

Office of Information and Technology (OIT)

eMASS ID #2031

Date PIA submitted for review:

November 18, 2024

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)	Randall Smith	Randall.Smith@va.gov	319-338-0581
Information System Owner	Shane Elliott	Shane.Elliott@va.gov	909-435-1808

Abstract

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

Application for Visit Summaries (AVS) is developed, owned, and maintained by the Veterans Health Administration (VHA) Office of the Chief Technology Officer (CTO). The purpose of the program is to promote patient-centered, care through enhancing communications, and engaging patients in their care. AVS summarizes medications, appointments, tests, patient education material and other instructions to improve recall of medical instructions. As many patients and clinicians have experienced, patients tend to forget most of what they are told during outpatient visits. In fact, patients forget 40% to 80% of the information from healthcare providers. Of what patients do remember, they remember about half incorrectly and the more information they are given, the less they remember. Moreover, patients desire more information than they typically receive about their illnesses and treatment plan. Poor retention of the treatment plan leads to non-adherence, medication errors, missed appointments and perceptions of miscommunication with the provider. Clinical summaries of outpatient visits are a means to provide patients with the information they need after a visit with their healthcare provider.

Overview

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

1 General Description

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

The convenience of AVS for the Veteran increases the operational efficiency of VA by decreasing staff call volumes and summarizations of Veterans' visits. AVS provides a technology.

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

VA-owned and VA-operated. AVS was developed entirely by the VA and is hosted and maintained on servers internal to the VA network. The name of the VA Administration is VHA, and the program office is the Office of the Chief Technology Officer

2. Information Collection and Sharing

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

AVS stores approximately unique Veteran, facility, and clinic settings, none of which is PII/PHI. AVS collects but does not store or retain any PII/PHI.

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

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

Application for Visit Summaries (AVS) is developed, owned, and maintained by the Veterans Health Administration (VHA) Office of the Chief Technology Officer (CTO). The purpose of the program is to promote patient-centered, care through enhancing communications, and engaging patients in their care. AVS summarizes medications, appointments, tests, patient education material and other instructions to improve recall of medical instructions. As many patients and clinicians have experienced, patients tend to forget most of what they are told during outpatient visits. In fact, patients forget 40% to 80% of the information from healthcare providers. Of what patients do remember, they remember about half incorrectly and the more information they are given, the less they remember. Moreover, patients desire more information than they typically receive about their illnesses and treatment plan. Poor retention of the treatment plan leads to non-adherence, medication errors, missed appointments and perceptions of miscommunication with the provider. Clinical summaries of outpatient visits are a means to provide patients with the information they need after a visit with their healthcare provider.

The federal government recognizes the importance of this form of communication since the clinical summary, known as the After Visit Summary, is part of the meaningful use criteria that determines reimbursements for electronic health record implementation to physicians and hospitals. The Veterans Administration (VA) through its open-source software development and an AVS would be needed to meet that certification. What is currently available as an AVS through VistA and the Computerized Patient Record System (CPRS) is not adequate due to terminology and formats that are neither patient-centered or patient-friendly. In previous studies, a printed After Visit Summary has been shown to enhance patient trust and confidence in their physician and contribute to patient satisfaction. Despite

the fact that combining oral and written information is more effective than using either oral or written information alone, a printed After Visit Summary may be anachronous to the trend towards electronic health records.

Personal Health Records (PHR)s provide patients with electronic access to their health record and may increase patient's engagement in their healthcare. However, while the use of PHR's is increasing, not all patients have access to them. In fact, most veterans have not registered for the VA's MyHealtheVet website and of those who have, only about 25% have full access to their records to include progress notes, prescriptions, secure messaging, and other personal health information. Even when patients have access to PHR, patients access the After Visit Summary more frequently than other information available to them. AVS has been selected by the Veterans Health Administration (VHA) Innovations Selection Board and approved by the Veterans Administration (VA) Undersecretary for Health to be funded for national deployment. The VA Loma Linda Healthcare System Informatics Team is working closely with the VA's Virtual Lifetime Electronic Record (VLER) program on national deployment including uploading the AVS to MyHealtheVet (MHV) and MHV Secure Messaging.

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

AVS consists of an application server and a database. The application server provides a front-end graphical user interface while the database is used to store only application settings. All information collected and used by AVS is pulled directly from VistA, Medication Image Library (MIL), and CDW. If an after-visit summary report is generated, AVS transmits the report back to VistA's Imaging database to be stored.

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

Yes

G. Is the system operated in more than one site to include primary and secondary site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?

AVS is available to any VA site with access to VistA and Computerized Patient Record System (CPRS).

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

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

AVS operates under the Privacy Act of SORN79VA10 AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, section 7301(a)." verify and provide here.

I. What is the SORN?

SORN 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)

J. SORN revisions/modification

No.

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

No

4. System Changes

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

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

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

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

Section 1. Characterization of the Information

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

1.1 Information collected, used, disseminated, created, or maintained in the system.

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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

- ☒ Name
- ☒ **Full** Social Security Number
- ☐ **Partial** Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a Different Individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account Numbers
- ☐ Certificate/License Numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Medications
- ☒ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Gender/Sex
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☐ Date of Death
- ☐ Business Email Address
- ☐ Electronic Data Interchange Personal Identifier (EDIPI)
- ☒ Other Data Elements (List Below)

Other PII/PHI data elements: Appointment Date/Time, Clinic Name, COVID-19 Vaccination Interest/Status, VA Clinician Names.

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

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

Phone number, name, appointment date/time, clinic name, full SSN, and clinician name are pulled directly from VistA. COVID-19 vaccination appointment or vaccination status comes from the CDW for vaccinations or vaccination appointments made within the VA.

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.

Commercial aggregators are not used. Information is collected from individuals and/or EHRs to provide information relevant to appointments.

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

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

AVS generates reports for AVS/CPRS users using information from a veteran's medical appointment.

1.3 Methods of information collection

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

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

AVS collects all necessary information using Remote Procedure Calls (RPC)s from VistA, MIL, and Krames On Demand.

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

Information is not gathered on a form.

1.4 Information checks for accuracy, and how often will it be checked.

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

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

AVS retrieves information from VistA in real-time. VistA is the system of record for patient information and appointments. This uniquely identifiable system information is used to ensure accuracy of processed information, however, AVS does not store any PII.

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?

Commercial aggregators are not used.

1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.

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

The authority to collect the information in AVS is derived from the VistA system. The VistA System, and the VistA instances operate under the authority of Veterans' Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), 304, and Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a).
Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191(Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full-text); 45 C.F.R.parts 160 and 164 (HIPAA Privacy and Security Rules).
- System of Record Notice - 79VA10 Veterans Health Information Systems and Technology Architecture – VA
  https://www.oprm.va.gov/docs/SORN/Current_SORN_List_05_09_2023.pdf

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The system collects & processes PII and PHI on Veterans and on Members of the Public. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal and financial harm to the individuals impacted and adverse negative effect to the VA.

Mitigation: Data collected & processed 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 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
Patient name	Identification purposes	Not used
Date of Birth	Identification purposes	Not used
Full Social Security Number	Identification purposes	Not used
Personal Mailing Address	Listed in after-visit summary report for informational purposes	Not used
Appointment Date/Time	Listed in after-visit summary report for informational purposes	Not used
Clinic Name	Listed in after-visit summary report for informational purposes	Not used
Gender/Sex	Listed in after-visit summary report for informational purposes	Not used
Medical Records	Listed in after-visit summary report for informational purposes	Not used
Medications	Listed in after-visit summary report for informational purposes	Not used
COVID-19 Vaccination Interest/Status	Listed in after-visit summary report for informational purposes	Not used
Clinician Name	Listed in after-visit summary report for informational purposes	Not used

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

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

AVS creates trend-analysis, and relational analysis reports utilizing PowerBI software to analyze and display the data analytics in the form of visual graphs and charts, as well as sums, averages. These reports do not contain any PII/PHI and are only accessible on the VA-network.

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.

AVS does not create or make available any new or previously utilized information regarding an individual Veteran.

2.3 How the information in the system is secured.
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

Access to the AVS is controlled by VistA access and VA Single Sign On Internal (SSOi). Only users with a VistA account may access AVS. In accordance with VA Directive Handbook 6210, all AVS users begin with the minimum level of access required to utilize the application. Additionally, AVS inherits VistA site access rules, ensuring each user can only access those Medical Center Electronic Health Records the user is authorized to access in VistA. The system owner is responsible for ensuring these safeguards are in place and functioning.

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

AVS user access to SSN is limited to the Medical Center Electronic Health Records (VistA) the user is authorized to access in VistA and are only displayed in specific reports.

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

Access to AVS is controlled by VistA access and VA Single Sign On Internal (SSOi). Only users with a VistA account may access the AVS portal. In accordance with VA Directive and Handbook 6210, all AVS users begin with the minimum level of access required to utilize the application. Additionally, AVS inherits VistA site access rules, ensuring each user can only access those Medical Center Electronic Health Records the user is authorized for in VistA.

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?

Access to AVS PII is controlled by VistA access and Single Sign On Internal (SSOi). Only Users with a VistA account may access AVS PII. In accordance with the VA Directive and Handbook 6210, all AVS Users with the minimum level of access required to utilize the application.

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

AVS inherits VistA site access rules, ensuring each user can only access those Medical Center Electronic Health Records the user is authorized for in VistA.

2.4c Does access require manager approval?

AVS inherits VistA site access rules, ensuring each user can only access those Medical Center Electronic Health Records the user is authorized for in VistA.

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

Yes, when an after-visit summary is loaded, it is logged in the AVS SQL Server.

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

The system owner is responsible for ensuring AVS safeguards are in place and functioning.

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*

AVS processes the following information: Name; Phone Number; Appointment Date/Time; Clinic Name; Last four of SSN; COVID-19 Vaccine Interest/Status. No information is stored; AVS generates a report and sends it to VistA's Imaging database.

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

AVS does not store or retain any PII/PHI. The AVS SQL Server is only used to save visual settings for facilities, clinics, and users.

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

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

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

Yes

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

AVS does not store/retain the information in the after-visit summary it creates.
For the data that is stored such as facility, clinic, and user settings, the following apply:
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 2100.32100.3, 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).

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.

Data no longer necessary will be deleted from the database. Data contained in AVS is transitory and is retained within VistA. This is in accordance with RCS 10–1, Item 2000.2, DAA–GRS–2013–0005–0004, item 020 and RCS10–1, Item 2100.32100.3, DAA–GRS–2013–0006–0004, item 31.

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.

Any information shared for research will be de-identified and will not include Name and Phone Number. This will ensure the information is no longer PII. Any information shared for research will be de-identified and will not include Name and Phone Number. This will ensure the information is no longer PII.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

Principle of Minimization: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

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

Follow the format below:

Privacy Risk: There is a risk that the information processed by AVS could be accessed by unauthorized personnel.

Mitigation: The AVS application ensures that all personnel involved with the collection and use of data are trained in the correct process for collecting and using this data. A Privacy Officer (PO) and an Information System Security Officer (ISSO) are assigned to the boundary to ensure their respective programs are understood and followed by all to protect sensitive information form the time it is captured by the VA until it is finally disposed of. Each of these in-depth programs have controls that overlap and are assessed annually to ensure requirements are being met and assist staff with questions concerning the proper handling of information.

Additionally, only personnel with the appropriate credentials and physical access to VistA workstations can authenticate to the application. AVS is internal to the VA with no external connections. Any after-visit summary report a patient requests is printed only upon request and given directly to the patient.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a AVS consists of 2 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 <**Information System Name**> and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) 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
Application Server	Yes	No	• Patient Name • Date of Birth • Social Security Number • Appointment Date/Time • Clinic Name • Gender • Medical Records • Medical History • Medications • Problem List • Diagnosis • Lab Results • Progress notes • Encounter Information • Vital Signs • Immunizations • Allergies • COVID-19 Vaccination Interest/Status	Provide clinicians and veterans with a summary after medical appointments and for reporting purposes.	• Username/ Password • PIV • Various levels of access • SSL encryption for transmission

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

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

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

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

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

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

Data Shared with Internal Organizations

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Veterans Health Administration VistA	AVS gathers necessary information from VistA to compile into an after-visit summary report	Phone number, Name, ICN, Appointment Date/Time, Clinic Name, Last four of SSN	Remote Procedure Calls (RPC)
Corporate Data Warehouse (CDW)	AVS gathers necessary information from CDW to compile into an after-visit summary report	Phone number, Name, ICN, Appointment Date/Time, Clinic Name, Last four of SSN, COVID-19 Vaccination Interest/Status	Extract Transform Load (ETL)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The internal sharing of data is necessary for individuals to receive benefits. However, there is a risk that the data could be shared with an inappropriate VA organization or institution which could result in a breach of privacy and disclosure of PII/PHI to unintended parties or recipients.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity.

Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc.***	***List the method of transmission and the measures in place to secure data***

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: Not applicable as there is no external sharing.

Mitigation: Not applicable as there is no external 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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non-Veterans receiving care are provided the notice at the time of their encounter.

This Privacy Impact Assessment (PIA) also serves as notice 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."

A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority and the conditions under which the information can be disclosed.

Notice is also provided in the Federal Register with the publication of the SORN: Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (79VA10).

6.1b If notice was not provided, explain why.

The routine use provision of the Privacy Act functions as one of the exceptions to the statute's general prohibition against the disclosure of a record without the written consent of the individual to whom the record pertains.

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

Notice is provided to all Veterans who are eligible for care. The notice is also available at all VA medical centers as well as online:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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 used is previously collected and stored in VistA. Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them. There is no penalty for opting out of providing information.

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.

AVS can include various data elements in an after-visit summary report. Patients will be presented with consent when a clinician asks them if they would like an after-visit summary report and have the option of opting out of receiving the report.

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.

Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their 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.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: This is referring to sufficient notice provided to the individual.

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

Privacy Risk: There is a risk that 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.

Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Practices (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 The procedures that allow individuals to gain access to their information.

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

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

The system does not create any new patient information that the patient does not already have access to through the medical records system. All information that the system obtains is already available in the patient's medical records (i.e., VistA).

SORN for 79VA10 (Veterans Health Information Systems and Technology Architecture (VistA) Records – VA) 2020-28340.pdf ***provides record access procedures:*** Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact.

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 subject to 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?

VistA is the electronic medical record database for VA and has an established process for release of information to obtain a copy of or make changes to information in VistA.

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.

The system does not create any new patient information that the patient does not already have access to through the medical records system. All information that the system obtains is already available in the patient's medical records (i.e., VistA). VistA is the electronic medical record database for VA and has an established process for release of information to obtain a copy of or make changes to information in VistA.

SORN for 79VA10 (Veterans Health Information Systems and Technology Architecture (VistA) Records – VA) 2020-28340.pdf ***provides record access and contesting procedures:*** Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact.

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.

The system does not maintain health records; records are maintained within VistA.

SORN for 79VA10 (Veterans Health Information Systems and Technology Architecture (VistA) Records – VA) 2020-28340.pdf ***provides record access and contesting procedures:*** Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact.

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.

The system does not maintain health records outside of VistA. Therefore, there would be no inaccurate or erroneous information to correct as it relates to AVS. This would be done within VistA.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: AVS obtains data from VistA. The risk of incorrect information in an individual's records is mitigated by authenticating information when possible. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.
The NOPP discusses the process for requesting an amendment to one's records.

The Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information.
The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

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

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

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

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

There are currently seven levels of access to the AVS Portal (the web interface used to access various functions of the system). All seven levels of access require that the user has an active VistA account and a VA PIV card and PIN for Two Factor Authentication (2FA) through VA SSO. ADMIN and VISN access must be requested by the existing Facility or VISN POC.

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?

Any hospitalist only internal to the VA that has access to VistA and CPRS can access AVS at the most basic permission level. Users from other government agencies only have access to AVS if they have a VistA account, otherwise, users from other government agencies do not typically have access to the application. Although out of AVS's scope, VistA accounts are only created when vetted users within the VA require it.

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.

User Types:

Elevated privileges for AVS users allow access to the AVS Admin Console, through which users may make configuration changes to the AVS. These privileges are granted on the basis of two VistA user classes:

AVS ADMINISTRATOR: allows access to all AVS settings

AVS BATCH PRINT: allows for setting up batch printing for clinics

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

Contractors will have access to the system and the PII/PHI only if their role requires access as part of their required duties. All contractors accessing the system are required to follow VA policies and procedures to obtain and maintain a VA Network account before accessing the AVS system.

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

Contractors may be involved in the design and development of future enhancements and/or maintenance and support of the system.

8.2c. Does the contractor have a signed confidentiality agreement?

The Contracting Officer Representative (COR) verifies contractor eligibility for VA network access including a favorable background investigation, signed NDA, and annual VA privacy training. If

access to CDW PII and PHI data is required, contractors will be required to complete the National Data Services (NDS) ePAS User Request process.

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

The Contracting Officer Representative (COR) verifies contractor eligibility for VA network access including a favorable background investigation, signed NDA, and annual VA privacy training. If access to CDW PII and PHI data is required, contractors will be required to complete the National Data Services (NDS) ePAS User Request process.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?

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.

The Contracting Officer Representative (COR) verifies contractor eligibility for VA network access including a favorable background investigation, signed NDA, and annual VA privacy training. If access to CDW PII and PHI data is required, contractors will be required to complete the National Data Services (NDS) ePAS User Request process.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Annual VA privacy training. Users are required annually to complete "VA Privacy and Information Security Awareness and Rules of Behavior" and "VA Privacy and HIPAA Training."

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

8.4a If Yes, provide:

1. *The Security Plan Status:* **Complete**
2. *The System Security Plan Status Date:* **October 24th, 2024**
3. *The Authorization Status:* **Assess Only**
4. *The Authorization Date:* **March 10th, 2022**
5. *The Authorization Termination Date:* **December 5th, 2025**
6. *The Risk Review Completion Date:* **March 10th, 2022**
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.***

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. ***(Refer to question 1.8 of the PTA)***

No; the system does not use cloud technology.

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). ***(Refer to question 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

N/A; AVS is not utilizing any Cloud Service Provider

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; AVS is not utilizing any Cloud Service Provider

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; AVS is not utilizing any Cloud Service Provider

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; AVS is not utilizing any RPA

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2024.12.20 15:08:08 -05'00'

Privacy Officer, Nancy Katz-Johnson

RANDALL SMITH

Digitally signed by RANDALL SMITH
Date: 2024.12.20 14:17:53 -06'00'

Information Systems Security Officer, Randall Smith

SHANE ELLIOTT

Digitally signed by SHANE ELLIOTT
Date: 2024.12.20 11:41:41 -08'00'

Information Systems Owner, Shane Elliott

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).

VHA NOPP: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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

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

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

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

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)