Privacy Impact Assessment for the VA IT System called:

VistA Audit Solution (VAS)

Veterans Health Administration (VHA)

Office of Information Technology (OIT)

Date PIA submitted for review:

08/24/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	(513) 721-1037
Information System Security Officer	Richard Alomar-Loubriel	Richard.Alomar-Loubriel@va.gov	787.696.4091

	Name	E-mail	Phone Number
Information System Owner	Tony Sines	Tony.Sines@va.gov	316.249.8510

Abstract

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

VistA Audit Solution (VAS) provides a nationwide Health Insurance Portability and Accountability Act (HIPAA) compliant Audit Tracking Solution with the ability to track and report on the who accessed any patient's PII/PHI data across all VistA instances. Currently, VAS end-users are Information Systems Security Officers (ISSO) and/or Privacy Officers, and/or their authorized representatives who need the ability to view the log of Create, Read, Update and/or Delete (CRUD) operations to respond to Freedom of Information Act (FOIA) requests from Veterans.

Overview

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

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

• The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission. • Indicate the ownership or control of the IT system or project.

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

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

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

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

• A citation of the legal authority to operate the IT system.

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

• Whether the completion of this PIA could potentially result in technology changes

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

VistA Audit Solution (VAS) is part of Veterans Health Administration (VHA). VistA Audit Solution (VAS) is an Internal only system. VAS is intended to provide a Health Insurance Portability and Accountability Act (HIPAA) compliant system for addressing potential HIPAA violations regarding the accessing of Personally Identifiable (PII) and Protected Health Information (PHI) of Veterans and

their dependents by unauthorized individuals. VAS will have the potential to access all veterans' records. According to the VHA, there are about nine million veterans' records documented as of the submission of this document which according to the VHA is about nine million. There are 152 VA medical Centers that host VistA. The system will be hosted at VA Enterprise Cloud-Amazon Web Service. (VAEC-AWS), AITC and PITC. The system will consist of a cluster of Redis Enterprise servers at VA Datacenters, communicating with a Node JS application, which will filter the data sent from VistA instances and push the data to a Data Repository in the VAEC AWS Cloud. Upon receipt of a potential HIPAA violation, authorized individuals will be able to query the Metadata Query Audit Retrieval Interface. There is only one-way information received from VistA. There will be no sharing conducted by VAS to any other IT system.

No business processes or technology changes are anticipated from the completion of this PIA.

- A citation of the legal authority to operate the IT system.

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

- *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?*

Currently VAS does not have a ATO this is a new system.
The ATO need date is planned for October 27, 2022.
IOC date: 03/22/2023

All essential artifacts and documents have been uploaded to eMASS accordance with the VA Directive 6500, VA 6500.3. VAS has legal authority to use the following:

- Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Part 160
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Privacy Act of 1974; U.S. Code title 5 USC section 301 title 38 section 1705, 1717, 2306-2308 & Title 38 US Code section 7301 (a) and Executive Order 9397
- The legal authority is 38 U.S.C 7681-7683
- OMB Memo Circular A-130, Management of Federal Information Resource, 1996
- OMB Memo M~~99-18, Privacy Policies on Federal Web Sites
- OMB Memo M~~03—22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
- Authority for Maintenance of the system – Public Law 93-43
- Title 38 United States Code, § 501
- 79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA

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?

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

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

Health Insurance

PII Mapping of Components

VAS consists of 1 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VAS and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (YES/NO)	Does this system store PII? (YES/NO)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII: Search History	Safeguards

AWS Redshift	**Yes**	**Yes**	**Personally Identifiable Information (PII), Protected Health Information Name, Social Security, Date of Birth, Personal mailing address, Personal email address, Medical record, Personal Phone number, Race and Ethnicity, Health Insurance Beneficiary Account numbers, and Financial Records, Emergency Contact Information (Name, Phone Number)**	**VistA Audit intend to provide HIPAA compliant system for addressing HIPAA violations with regard to the accessing PII and PHI Veterans and dependents information unauthorized**	**Stored in an encrypted database and only accessible by authorized users.**

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

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? 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 1.3 indicate why the system is using this source of data. If the system creates information (for example, a score, analysis, or report), list the system as a source of information. This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent

VistA Server instances within the VA will provide Veterans and dependents name, Social Security numbers, date of birth, personal mailing address, personal email address, medical record, phone number, race and ethnicity, personal phone number, mother's maiden name, employer name, employment status, date of death, financial records, health insurance beneficiary numbers, account numbers, and emergency contact information (name, phone number, etc.).

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number. This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information is sent by VistA and collected by a Redis Enterprise Message queue service and transmitted over a secure connection to an offsite data repository hosted in the VAEC GovCloud. The data can then be displayed on the end user interface, in response to the specific query entered.

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

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. If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract. This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

VAS does not check for any accuracy or corruption of information that is being transmitted from VistA instances across the VA. The information collected from VistA is only presumed to be correct when information is transferred from VistA to Redis and custom Node JS application to a Data Repository in the VAEC GovCloud.

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

- Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Part 160
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Privacy Act of 1974; U.S. Code title 5 USC section 301 title 38 section 1705, 1717, 2306-2308 & Title 38 US Code section 7301 (a) and Executive Order 9397
- The legal authority is 38 U.S.C 7681-7683
- OMB Memo Circular A-130, Management of Federal Information Resource, 1996
- OMB Memo M~~99-18, Privacy Policies on Federal Web Sites
- OMB Memo M~~03—22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
- 79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA
- Authority for Maintenance of the system – Public Law 93-43
- Title 38 United States Code, § 501

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: If the PII/PHI system information collected and retained were accessed by an unauthorized individual or otherwise breached, then personal and/or emotional harm or even identity theft may result.

Mitigation: Single Sign On using PIV access for authorized users only is permitted. Authorized users are Privacy Officers (PO) and Information System Security Officers (ISSO) and their authorized representatives. The authorized VAS users will be able to view who accessed the patient data and if data was modified, and if so, what data was modified.

Section 2. Uses of the Information

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

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

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

The information will be used to provide a quarterly report on Health Insurance Portability and Accountability Act (HIPAA) compliance to Congress and provides reports as needed by the Surgeon General. To address potential HIPAA violations regarding the accessing of Personally Identifiable Information (PII) and Protected Health Information (PHI) of Veterans and their dependents by unauthorized individuals. There are NO external users of the VAS system.

•SSN –Veteran/Patient identification and Audit log purposes
•Patient Date of Birth –Patient Identification and Audit log purposes
•Mailing Address –Contact and correspondence with patient and Audit log purposes
•Zip Code-part of the mailing address and Audit log purposes
•Phone Number(s) –Contact and correspondence with patient and Audit log purposes
•Emergency Contact Information -Contact and correspondence with patient's next of kin
•Previous Medical Numbers –Used to track who few the records and Audit log
•Patient Race/Ethnicity –statistical reporting and Audit log purposes
•Health Insurance Beneficiary Account Numbers – Audit log purposes and to see who viewed the info

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

Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in,

among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

VAS is used to track who in the VA has accessed an individual's health record within VistA.

2.3 How is the information in the system secured?

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

The data from VistA is sent over encrypted tunnels using Advance Encryption Standard (AES) and VAS employs standard data communication ports and Secure Sockets Layer (SSL) based connected to transmit any data with the internally hosted systems (within the VA network). Once the data is in the VAS system it is encrypted within the Database. Encryption in transit and at rest is performed as required for both the on-prem and cloud environments.

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

However, due to the nature of the system the full SSN must be shown on the screen to verify it is correct. All data in flight are fully encrypted utilizing Transport Layer Security (TLS) and FIPS 140-2 and encrypted database are used for data at rest.

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

Stored and transmitted PII/PHI is safeguarded with encryption and no data leaves VA controlled environments.
To protect Veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:
1. The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while, used developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.

4. Internal protection is managed by access controls such as user IDs and passwords, two-factor authentication, in addition: awareness and training, encryption, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC28, Protection of Information at Rest

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Add answer here:

VAS is used to verify who accessed PII/PHI information within VistA. The Privacy Officer (PO), Information System Security Officer (ISSO) and their authorized representatives have access to the system and to view data as part of auditing, monitoring, and privacy review as needed.

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

Veterans and dependents name, Social Security Number, date of birth, personal mailing address, personal email address, medical record, phone number, race and ethnicity, personal phone number, mother's maiden name, employer name, employment status, date of death, and financial records, health insurance beneficiary numbers, account numbers, and emergency contact information (name and phone number).

3.2 How long is information retained?

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

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

System Access Records for VAS will be retained for 6 years in accordance with Records Control Schedule (RCS 10-1 for access data). Data aged past the retention schedule will be deleted by a monthly process. This expired data will not be archived.

- VA Directive 6300 Records and Information Management September 18, 2018
- 79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA

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

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

The data retention period has been approved by NARA and is processed according to the following:

- Records Control Schedule 10-1 link for VHA: www.va.gov/vhapublications/rcs10/rcs10-1.pdf National Archives and Records Administration – www.nara.gov
- The VAS program team performs an annual review to ensure compliance with the requirements.
- In accordance with System Access Records 2100.3 DAA-GRS-2113-0006-0003, ITEM 030

3.4 What are the procedures for the elimination of SPI?

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

Records/digital information will be eliminated following the sanitization procedures in VA Handbook 6300.1 Records Management Procedures and VA Handbook 6500.1 Electronic Media Sanitization. Schedule 3.0 and 4.0, approved by National Archives and Records Administration (NARA).

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research? This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

For testing and training, a pre-production and development site has been set-up.VAS uses test patient or fictitious information for testing, training, and research.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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

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

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

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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: If transaction growth rates exceed expectations during the retention schedule, then storage capacity may be exceeded, and the integrity of the data will degrade. System Access Records for VAS will be retained for 6 years in accordance with Records Control Schedule (RCS 10-1 for access data). If data is not retained, Veteran's and VA employees will not have the ability to find out who accessed their PII/PHI information.

Mitigation: System monitoring is used to consistently monitor data storage capacities and growth rates. Additional budget and minimal system administration are required to increase storage and ensure proper disposal of data according to the retention schedule.

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***
Veterans Health Information Systems and Technology Architecture (VistA)	Information is used to audit who access the PII/PHI records	Name, Social Security Number, date of birth, personal mailing address, personal email address, medical record, personal phone number, race and ethnicity, health insurance beneficiary account numbers, and financial records, emergency contact information (name and phone number)	FIPS 140-2 Encrypted TCP

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Follow the format below:

Privacy Risk: If information is inadvertently shared with individuals who may not have a need to know, then data could be compromised at the time of transmission.

Mitigation: VAS employs encryption at transit and at rest. Insider data corruption/compromise due to inadvertent data share and/or spillage is mitigated in accordance with VA processes and procedures and falls outside the prevue of VAS. VAS employs standard data communication ports and secure (SSL) based connected to transmit any data with these internally hosted (within the VA network) systems.

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.

VAS will not share data with any external organization or system.

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	

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

Section 6. Notice

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

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

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

VAS is a read-only system. Data comes from VistA instances across the VA. Veterans are already notified via the Notice of Privacy Practice (NOPP). The NOPP explains the collection and use of protected information to individuals applying for VHA benefits. The Veteran is notified of how VA may use their information without authorization and instances when an authorization is required from the Veteran. The NOPP is given out when the Veteran enrolls or when updates are made to the NOPP. Copies of the NOPP are mailed to all VHA beneficiaries.

https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=3147

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

Within VAS individuals do have the ability to decline providing information as the data comes from VistA instances across the VA. A Veteran at the point of care has the right to decline to provide VA information. This right is described in the NOPP and may be exercised at the point of care. VAS captures information entered in VistA.

6.3 Do individuals have the right to consent to particular use 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 permits individuals to agree to the collection of their personally identifiable information (PII) using paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used, and what Privacy Act system of records the information will be stored. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA Notice of Privacy Practices. VHA uses PII and PHI only as legally permitted including obtaining authorizations where required. Where legally required VHA obtains signed, written authorizations from individuals prior to releasing, disclosing, or sharing PII and PHI. Individuals have a right to restrict the disclosure and use of their health information.

Individuals who want to restrict the use of their information should submit a written request to the facility Privacy Officer where they are receiving their care.

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.

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: There is risk that a Veteran may not know how to request access to the VAS data and that the data exists as it does in the VistA environment.

Mitigation: VA SORN, 79VA10 describes the data collected and how the Veteran may request a copy of the data and audit log available in the system.
https://www.oprm.va.gov/docs/Current_SORN_List_7_1_2022.pdf

Section 7. Access, Redress, and Correction

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

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

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

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

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

The individual/Veteran must submit a signed written request for a copy of the data in VAS to the facility where they receive treatment. The request may be submitted to the local Privacy Officer. This process is also described in the VA SORN 79VA10, the NOPP and within VHA Directive 1605.01.

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.

VAS is a read only system capturing data from VistA. An individual/Veteran who wishes to request an amendment must submit a request to the local facility Privacy Officer. The process for submitting an amendment request is reflected in the NOPP and within VHA Directive 1605.01.

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.

Veterans are informed of the amendment process in the NOPP which states:

> **Right to Request Amendment of Health Information.**
> You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.
> If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:
> - File an appeal
> - File a "Statement of Disagreement"
> - Ask that your initial request for amendment accompany all future disclosures of the disputed health 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. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

Veterans are informed of the amendment process through the NOPP.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

This question is related to privacy control IP-3, Redress.

Follow the format below:
Privacy Risk: There is a risk that a Veteran may not know how to obtain access to their records or how to request corrections to their records.

Mitigation: The NOPP, which every patient receives when they enroll for care, discusses the individual rights of access, redress and correction of records. VHA staff distributes a Release of Information (ROI) process at the VA facilities to assist Veterans with obtaining access to their health records and other records containing personal information. In addition, VHA Directive 1605.01, establishes procedures for Veterans to request copies of their records, review their records and request an amendment of their records.

Section 8. Technical Access and Security

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

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

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

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

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

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

Users will submit an ePASS request to have the correct user groups tied to their account. All user accounts are read only.

Administrator accounts for on premise (AITC/PITC) will submit an ePASS request; this will be used with their zero token and 2FA for log in.

For AWS access administrators will submit request to ePASS to be added to the AWS groups, then submit a request to the VA COMS team for access to the correct portal.

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.

All contractors have signed Contractor Rules of Behavior and Non-Disclosure Agreement. Contractors complete appropriate background investigations and have received security clearance in accordance with VA Standard Policies and Procedures needed to perform their tasks; and complete VA Privacy and Information Security Awareness and Rules of Behavior training, and the VHA Privacy and HIPAA training, and are re-certified annually.

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.

Personnel (contractor support, PO, ISSO, and their authorized representatives) who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security

awareness training which all personnel must complete via the VA's Talent Management System 2.0 (TMS 2.0). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS 2.0 system. All VA employees must complete annual Privacy and Security training. This training includes the following TMS 2.0 Courses:

- VA 10176: Privacy and Info Security Awareness and Rules of Behavior
- VA 10203: VHA Privacy and HIPAA Focused Training

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

If Yes, provide:

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

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

No – VAS does not currently have an Authority to Operate (ATO); the Initial Operating Capability (IOC) date is scheduled to be completed 03/22/2023. The system classification is at a moderate.

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).

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.

VAS system is using AWS-VAEC. VAS is using a mix of Infrastructure as a Service (IaaS) and Software as a Service (SaaS) for the system.

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)

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

N/A – The contract is between VA and AWS and the system does not have access to those documents.

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 – The contract is between VA and AWS and the system does not have access to those documents.

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

ID	Privacy Controls
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.

Phillip Cauthers 255139

Digitally signed by Phillip Cauthers 255139
Date: 2022.09.07 15:01:38 -07'00'

Privacy Officer, Phillip Cauthers

RICHARD ALOMAR-LOUBRIEL 139039

Digitally signed by RICHARD ALOMAR-LOUBRIEL 139039
Date: 2022.09.07 18:40:44 -04'00'

Information Systems Security Officer, Richard Alomar-Loubriel

Tony L. Sines 167047

Digitally signed by Tony L. Sines 167047
Date: 2022.09.07 15:15:51 -05'00'

Information Systems Owner, Tony Sines

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms).

System of Records Notice

- 79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA

- https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

VHA Notice of Privacy Practices

- https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=3147