Privacy Impact Assessment for the VA IT System called:

VistA Adaptive Maintenance (VAM)

Enterprise Cloud Solutions Office (ECSO)
Veterans Health Administration

Date PIA submitted for review:

8/24/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	nancy.katz-johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Albert Estacio	albert.estacio@va.gov	909-583-6309
Information System Owner	David Catanoso	david.catanoso@va.gov	732-740-9708

Abstract

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

The VistA Adaptive Maintenance (VAM) system is a comprehensive, commercial Cloud-First/Cloud Native security solution that provides security for all remote clients, applications, and users of VistA data via monitoring and securing VistA's Remote Procedure Call (RPC) interface within the VA's FedRAMP high Enterprise Cloud (VAEC).

Overview

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

1 General Description

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

VistA Adaptive Maintenance (VAM), VAEC

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

VistA Adaptive Maintenance (VAM) is a Cloud-Smart / Cloud-Native application deployed in the dedicated U.S. FedRAMP-HIGH, HIPAA-compliant VA Enterprise Cloud (VAEC) leveraging Amazon Web Services (AWS) commercial cloud infrastructure, security, and services. VAM is a passive monitoring system which sends the log of VistA traffic to AWS CloudWatch Logs for security monitoring. Some of this VistA traffic may contain PII. AWS CloudWatch Logs is FedRAMP-high certified and stores all data in encrypted form within the FedRAMP-high, HIPAA-compliant VAEC VAM provides comprehensive, commercial cloud-based monitoring and security for all remote clients, applications, and users that access VistA data via VistA's Remote Procedure Call (RPC) interface. VAM is operationalized and scaled for production enterprise's use in the VAEC leveraging FedRAMP-high approved AWS Kinesis Streams and AWS CloudWatch Logs and provides comprehensive commercial cloud-based VistA RPC Interface monitoring and security for all VistA systems migrated to the VAEC. VAM is 100% Legacy-free, Cloud-Native, and Non-invasive - allowing it to be scaled and deployed enterprise-wide without any change required for any VistA system or any end-user Client or Application. VAM does not allow for connection or sharing of information in identifiable form with external organizations, websites or applications. VAM will be hosted in production within the VA's FedRAMP-high / HIPAA certified Enterprise Cloud (VAEC) using Amazon Web Services (AWS).

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

VA Owned and VA Operated e provide response here

2. Information Collection and Sharing

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

VistA is the source information. The VAM application / RPC Mirror and RPC Monitor are not an End User based software and there is no GUI (Graphical User Interface). VAM is a passive monitoring system that sends the mirrored client-to-VistA RPC traffic to an alternate, data streaming service (AWS Kinesis), which sends the log of VistA traffic (Data source) to Amazon Web Services (AWS) AWS CloudWatch Logs for security monitoring. VistA traffic contains varying levels of PII. AWS CloudWatch Logs is FedRAMP-high certified and stores all data in encrypted form within the FedRAMP-high, HIPAA-compliant VAEC.

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

VAM mirrors the traffic from all remote Clients (such as CPRS) that use VistA's Remote Procedure Call (RPC) interface and stores this traffic log in encrypted form in the FedRAMP-high certified AWS. CloudWatch Logs within VAEC. This is a fully automated process. There is no human involvement in the capture or management of any of this data. All information is fully and immediately encrypted within AWS CloudWatch Logs. There is no access to any of the traffic logs outside of the Virtual Private Network (VPN) of the VAEC. Purpose is to provide monitoring for all remote clients, applications, and users that access VistA data via VistA's Remote Procedure Call (RPC) interface.

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

VAM application and RPCs do not store or transmit any information outside the VAEC network. The RPC Mirror and RPC Monitor logs, describes, and classifies Vista data and migrates (by Executive Order 9397) it to AWS Kinesis Streams and AWS CloudWatch Logs located in AWS VAEC.

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

VAM application and RPCs do not store or transmit any information outside the VAEC network. The RPC Mirror and RPC Monitor logs, describes, and classifies Vista data and migrates (by Executive Order 9397) it to AWS Kinesis Streams and AWS CloudWatch Logs located in AWS VAEC.

3. Legal Authority and SORN

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

Executive Order 9397 allows Federal agencies to collect and use the SSN. VAM will migrate information collected to support the EHR from legacy systems to a secure, centralized, cloud-based system. All processes in place for the legacy systems will remain in place during migration of data. VAM is hosted in the VAEC environment and at High Assessing, the information that is logged is done so in AWS CloudWatch Logs that also resides in the AWS VAEC, thus the collection of data/data retention is inherited through the Cloud Service Provider (CSP) in accordance with the Customer Responsibility Matrix (CRM).

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

NA

D. System Changes

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

NA

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

NA

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☒ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☒ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☒ Certificate/License numbers*
- ☒ Vehicle License Plate Number
- ☒ Internet Protocol (IP) Address Numbers
- ☒ Medications
- ☒ Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number

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

VAM application and RPCs do not store or transmit any information outside the VAEC network. The RPC Mirror and RPC Monitor logs, describes, and classifies Vista data and migrates (by Executive Order 9397) it to AWS Kinesis Streams and AWS CloudWatch Logs located in AWS VAEC. Other information that will be accessed and processed include:

- Gender
- Guardian name and contact information
- Next of kin name and contact information
- Military and service history
- Employment information
- Veteran dependent information
- Education information
- Research medical statistics
- Service-connected rating and disabilities
- Criminal background information
- Date of death

PII Mapping of Components (Servers/Database)

VAM System creates no records, for any individual. The system just gathers general information of RPC transactions and stored them for further analysis, such analysis is not yet implemented does not contain a Database.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
AWS CloudWatch Logs	Yes	Yes	Patient demographic information, Patient healthcare information, lab orders/results, radiology orders/results, pharmacy order/results, procedures,	Parsing data and classifying it	AWS VAEC

			clinical notes, vitals, allergies, problems, clinical user data, ordering clinician. All data that can pass into and out of the CPRS application is passes from the client to the target.		
AWS Kinesis Streams	Yes	No	Patient demographic information, Patient healthcare information, lab orders/results, radiology orders/results, pharmacy order/results, procedures, clinical notes, vitals, allergies, problems, clinical user data, ordering clinician. All data that can pass into and out of the CPRS application is passes from the client to the target.	Mirrors Vista traffic	AWS VAEC

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

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

VistA is the source information. The VAM application / RPC Mirror and RPC Monitor are not an End User based software and there is no GUI (Graphical User Interface). VAM is a passive monitoring system that sends the mirrored client-to-VistA RPC traffic to an alternate, data streaming service (AWS Kinesis), which sends the log of VistA traffic (Data source) to Amazon Web Services (AWS) AWS CloudWatch Logs for security monitoring. VistA traffic contains varying levels of PII. AWS CloudWatch Logs is FedRAMP-high certified and stores all data in encrypted form within the FedRAMP-high, HIPAA-compliant VAEC.

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.

The system described in the previous sections, which includes the VAM application and RPCs, does not mention accessing a commercial aggregator of information for accuracy checking. Therefore, the process and accuracy levels required by the contract in this context are not applicable to the current system.

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

The system described in the previous sections, does not create information such as scores, analysis, or reports. Therefore, this question is out of context and not applicable to the current system.

1.3 How is the information collected?

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

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

VAM mirrors the traffic from all remote Clients (such as CPRS) that use VistA's Remote Procedure Call (RPC) interface and stores this traffic log in encrypted form in the FedRAMP-high certified AWS CloudWatch Logs within VAEC. This is a fully automated process. There is no human involvement in the capture or management of any of this data. All information is fully and immediately encrypted within AWS CloudWatch Logs. There is no access to any of the traffic logs outside of the Virtual Private Network (VPN) of the VAEC. Purpose is to provide monitoring for all remote clients, applications, and users that access VistA data via VistA's Remote Procedure Call (RPC) interface.

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

NA

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

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

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

All information passing into the VAEC environment has already been through the VA Network's authentication process. For the VAM Application itself, an RPC (Remote Procedure Call) is an American Standard Code Information Interchange (ascii) encoded message sent by VistA Clients to VistA over TCP connections. RPCs are logged and classified.

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

The system described in the previous sections, which includes the VAM application and RPCs, does not mention accessing a commercial aggregator of information for accuracy checking. Therefore, the process and accuracy levels required by the contract in this context are not applicable to the current system. It's important to note that the system's primary purpose is to provide monitoring and security for remote clients, applications, and users accessing VistA data via VistA's Remote Procedure Call (RPC) interface. The system's focus is on logging and securing the transmitted data within the VAEC network rather than checking information accuracy through a commercial aggregator

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

Executive Order 9397 allows Federal agencies to collect and use the SSN. VAM will migrate information collected to support the EHR from legacy systems to a secure, centralized, cloud-based system. All processes in place for the legacy systems will remain in place during migration of data. VAM is hosted in the VAEC environment and at High Assessing, the information that is logged is done so in AWS CloudWatch Logs that also resides in the AWS VAEC, thus the collection of data/data retention is inherited through the Cloud Service Provider (CSP) in accordance of the Customer Responsibility Matrix (CRM

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

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

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

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: VAM has been categorized in the Enterprise Program Management Office (EPMO) System Security Categorization as a High impact system based on the sensitive and important nature of the VistA data traffic that the VAM application monitors. The inherent risk from the VAM application is VistA traffic interruption. This can cause delays in day-to-day functions from providers. However, the risk of information exposure is based on the VAEC security maintaining integrity.

Mitigation: There are no connections outside of the VAEC to websites, or systems and does not directly collect information from individuals. VAM provides security monitoring for all remote access clients (CPRS, JLV, CAPRI, …) of all veterans' health and benefits information in the Veterans Information System and Technology Architecture (VISTA) systems. Additionally, system Log files, sample clinical data that may contain Protected Health Information (PHI) appropriate to the agreements. Veteran, veteran's primary contact and volunteer's service, medical, criminal record, guardian, education, and benefit information may be collected as well as contractor and employee personnel and payroll records may be collected and processed. The inherent risk from the VAM application is VistA traffic interruption. This can cause delays in day-to-day functions from providers. However, the risk of information exposure is based on the VAEC security maintaining integrity.

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.

VAM is meant to plan, develop, design, integrate, test, implement, and manage centralized services to provide comprehensive, real-time, 24/7 monitoring and security for all Veteran data in all VistA systems migrated to VAEC. VAM is a data-driven, minimally invasive, intelligent auditing and alerting classifier system of RPC inquiries into the VistA. As VA continues to strengthen its cybersecurity profile, project VAM will provide the following benefits. •Reduce the cost and complexity of the maintenance of VistA systems. Resolve security vulnerabilities of all VistA systems migrated to VAEC •Full utilization of the scaling and features of VA's commercial cloud capabilities •Ensure the safe, secure, and seamless continuity of Veteran care and services as VistA systems are migrated to VAEC. VAM Data will be used for data analysis.

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

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

VAM is comprised of three major architectural components, the RPC Monitor, the RPC Mirror, and the RPC Definition Models. Because VAM only resides in the VAEC environment, all other tools are inherited through the VAEC and Cloud Service Provider (CSP). 1. The RPC Monitor represents the software pipeline that facilitates RPC parsing, classification, and alert notification functions of the VAM application 2. The RPC Mirror represents the software that mirrors client-to-VistA RPC traffic to an alternate, data streaming service, Amazon Web Services (AWS) Kinesis. AWS Kinesis must make as small an impact as possible, as it sits on the critical network traffic path between VistA clients and VistA. 3. The RPC Definition Models represent the static RPC definition model files, generated by the RPC Definition Toolkit, and the classifier pipeline, resident in the RPC Monitor, that applies the models against RPC traffic to generate classifications and alerts. 4. NOTE: All of the VAM architectural components will be managed within a single security boundary in VAEC. VAM enables VA to transition from VistA systems to a single, secure, commercially managed set of centralized cloud-based services - Veteran Integrated Care Services (VICS) - while maintaining full backwards-compatibility and continuity of care and workflows of the Computerized Patient Record System (CPRS). VAM will be hosted in production within the VA's Enterprise Cloud (VAEC) using Amazon Web Services (AWS). The result of integration will streamline and improve patient care for Veterans and their dependents. No information is stored or handled outside the VAEC network. There is no connection outside of the VA to websites, or systems. VAM is not an End User based software and there is no GUI (Graphical User Interface).

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.

This is not part of the system's current functionality

2.3 How is the information in the system secured?

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

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

The VAM system employs robust security measures to protect data both in transit and at rest. These measures are designed to ensure the confidentiality, integrity, and availability of sensitive information, including PII/PHI. The following measures are in place: Data in Transit: Encryption Protocols: All data transmitted between system components and external systems is encrypted using strong encryption protocols such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL). These protocols establish secure and encrypted communication channels to prevent unauthorized interception of data during transmission. Secure Communication Channels: The VAM system enforces the use of secure communication channels for all data transmission. This includes communication between client systems, servers, and external services. Certificate-Based Authentication: Mutual authentication using digital certificates is implemented to verify the identity of both the server and the client during data transmission. This helps prevent man-in-the-middle attacks and ensures secure communication. Data at Rest: Encryption of Storage: Sensitive data, including PII/PHI, stored within the system's storage components, such as Amazon S3 buckets, is encrypted at rest. This encryption ensures that even if unauthorized access to storage occurs, the data remains unreadable without the appropriate decryption keys. Strong Encryption Algorithms: Industry-standard encryption algorithms and cryptographic methods are employed to secure data at rest. Advanced encryption algorithms like Advanced Encryption Standard (AES) with strong key lengths are commonly used. Key Management: Proper key management practices are implemented to ensure the security of encryption keys. Keys are stored separately from the data they encrypt, and access to keys is tightly controlled to prevent unauthorized decryption. Access Controls: Role-based access controls and permissions are applied to restrict access to stored data. Only authorized personnel with a legitimate need are granted access to sensitive information. Data Masking: For non-production environments or scenarios where real PII/PHI is not required, data masking techniques may be used. This involves substituting sensitive data with fictional or scrambled data to minimize exposure of actual PII/PHI. Regular Security Audits: Periodic security audits and assessments are conducted to ensure that encryption mechanisms remain effective and up to date. Any vulnerabilities or weaknesses are identified and addressed promptly. By implementing these measures, the VAM system ensures that data remains secure both in transit and at rest. These measures adhere to industry best practices and compliance standards to safeguard sensitive information against unauthorized access, interception, and data breaches.

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

Given the sensitivity of Social Security Numbers (SSNs), the VAM system has implemented specific additional protections to ensure the security and privacy of SSNs. These protections are designed to mitigate the risks associated with the collection, processing, and retention of SSNs, and they include the following measures: Strict Access Controls: Access to SSNs within the VAM system is strictly controlled and limited to authorized individuals with a legitimate business need. Role-based access controls are enforced to ensure that only those individuals who require access can view or manipulate SSNs. Encryption of SSNs: SSNs are encrypted both during transmission and while at rest. Strong encryption algorithms are used to protect SSNs from unauthorized access or interception. This encryption ensures that even if there's a breach or unauthorized access to the data storage, the SSNs remain encrypted and unreadable. Monitoring and Auditing: The system implements continuous monitoring and auditing mechanisms to detect any unauthorized access or unusual activities related to SSNs. These mechanisms help in identifying potential security breaches or unauthorized attempts to access SSN data. Data Retention Policies: SSNs are subject to strict data retention policies that determine how long they are stored within the system. Once SSNs are no longer required for the system's legitimate purposes, they are promptly and securely deleted. Regular Security Assessments: The system undergoes regular security assessments and reviews to identify vulnerabilities and potential risks related to SSNs. Any findings are addressed promptly to maintain the security of SSN data.

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

PII/PHI safeguarding in accordance with OMB Memorandum M-06-15 involves a comprehensive set of security measures and practices to ensure the protection of sensitive information. The VAM (VistA Adaptive Maintenance) system adheres to these guidelines through the following measures: Access Controls: Access to PII/PHI within the VAM system is restricted to authorized personnel only. Role-based access controls are enforced, ensuring that individuals can only access the data necessary for their roles. User authentication mechanisms, such as strong passwords and multi-factor authentication, are employed to prevent unauthorized access. Encryption: PII/PHI is encrypted both in transit and at rest. Data transmitted between system components and external systems is encrypted using industry-standard protocols (e.g., TLS). Data stored within the system's storage components, such as S3 buckets, is also encrypted to prevent unauthorized access. Auditing and Monitoring: The system implements robust auditing and monitoring mechanisms to track access and activities involving PII/PHI. Logs are generated and retained, allowing for the detection of unauthorized or suspicious activities. Regular reviews of logs are conducted to ensure the security of the information. Physical Security: The physical infrastructure that hosts the VAM system is maintained within a controlled and secure environment. Physical access to data centers and server rooms is restricted to authorized personnel only. Security Training and Awareness: All personnel who handle PII/PHI receive regular security training and awareness programs. This ensures that individuals are educated about proper data handling procedures, security best practices, and the importance of safeguarding sensitive information. Incident Response: The system has a well-defined incident response plan in place. In the event of a security incident or data breach, appropriate measures are taken to mitigate the impact, investigate the incident, and prevent similar occurrences in the future. Secure Development Practices: The development and maintenance of the VAM system follow secure coding practices. Vulnerability assessments and penetration testing are conducted regularly to identify and address potential security weaknesses. Data Retention and Disposal: PII/PHI is retained only for the required period, as outlined in the data retention policy. When data is no longer needed, secure disposal methods are employed to ensure that the information cannot be recovered. Data Minimization: The principle of data minimization is followed, ensuring that only the necessary

PII/PHI is collected and retained. Reducing the amount of sensitive information minimizes the potential impact in case of a security breach. By implementing these measures and aligning with OMB Memorandum M-06-15, the VAM system ensures the confidentiality, integrity, and availability of PII/PHI, thereby safeguarding the privacy of individuals and complying with federal security requirements.

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?

Only VA accredited staff have access to instances in the VA Enterprise Cloud (VAEC) and data on a per protocol basis. List of approved personnel is maintained in Data Access Request Tracker (DART) system on prem. An Institutional Review Board (IRB) has oversight for each protocol. All activity is pre-approved by local privacy officer and the Information System Security Officer (ISSO). This system uses Federal Information Security Management Act (FISMA) standard processes for approving and monitoring access. This system is continually monitored and audited for compliance to FISMA security standards.

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

Yes, criteria procedures and controls are documented within respective DART and IRB processes. The VAM Access Control Standard Operating Procedure (SOP) documents the criteria and responsibilities regarding access.

2.4c Does access require manager approval?

Yes, all activity is pre-approved by local privacy officer and ISSO

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

The VAM system uses centralized logging system (CLS) to monitor and log information. AWS CloudTrail is used to track and record. This system is continually monitored and audited for compliance to FISMA security standards.

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

The VAM Information System Owner (ISO) is responsible for safeguarding the PII

Section 3. Retention of Information

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

3.1 What information is retained?

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

All clinical and administrative data that passes through the RPC Broker port to include.
Name
Social Security Number
Date of Birth
Mother's Maiden Name
Personal Mailing Address
Personal Phone Number(s)
Personal Fax Number
Personal Email Address
Financial Information
Health Insurance Beneficiary Numbers Account numbers
Certificate/License numbers
Vehicle License Plate Number
Internet Protocol (IP) Address Numbers
Medications
Medical Records
Race/Ethnicity

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. The VA records officer should be consulted*

early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.

All RPC mirrored data is stored in S3 buckets in unstructured format for 15 days.

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

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

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

Yes, records retention and destruction comply with the NARA approved Records Control Schedule, RCS-10.

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

VAM is a passive monitoring system which sends the log of VistA traffic to AWS CloudWatch Logs for security monitoring with its record retention falling under 1004-Records Management Records with a Records Management Record item number of 1004.1 from the Records Control Schedule RCS 10-1, and a records description of "Tracking and Control Records". The Tracking and Control Records Disposition Authority number is DAA-GRS-2013-0002-0016 and the Disposition Instructions are: Temporary. Destroy when no longer needed, which for the VAM system has been determined to be 15 days. Link to the Request for Records Disposition Authority DAA-GRS-2013-0002-0016:

https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs-2013-0002_sf115.pdf

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

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

Once they reach 15 days they are automatically deleted daily.

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.

VAM does not have any external connections outside the VAEC environment. All data privacy restrictions are through the VAEC.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: VAM has been categorized in the EPMO System Security Categorization as a High impact system based on the sensitive and important nature of the VistA data traffic that the VAM application monitors. The inherent risk from the VAM application is VistA traffic interruption. This can cause delays in day-to-day functions from providers. However, the risk of information exposure is based on the VAEC security maintaining integrity.

Mitigation: VAM is hosted in the VAEC environment. Data retention requirements are inherited from the Cloud Service Provider (CSP) as identified in the Customer Responsibility Matrix (CRM) Per the VA 6500 and 6510, all members are provided required annual security awareness training. All members are required to review and sign a Rules of Behavior form, NDA (Non-disclosure agreement) and conduct TMS based trainings.

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***
Amazon Kinesis : Traffic mirror Vista-Prod client	VAM Data is for VAM SME use only and will be used for data analysis.	Patient demographic information, Patient healthcare information, lab orders/results, radiology orders/results, pharmacy order/results, procedures, clinical notes, vitals, allergies, problems, clinical user data, ordering clinician. All data that can pass into and out of the CPRS application	Amazon Kinesis – Data Streaming Service

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*
		is passes from the client to the target.	
Amazon Kinesis : Traffic mirror Vista-Prod target	VAM Data is for VAM SME use only and will be used for data analysis.	Patient demographic information, Patient healthcare information, lab orders/results, radiology orders/results, pharmacy order/results, procedures, clinical notes, vitals, allergies, problems, clinical user data, ordering clinician. All data that can pass into and out of the CPRS application passes from the client to the target.	Amazon Kinesis – Data Streaming Service
Traffic Mirror Monitor (4) Oma-az1 prod VCB-az1 prod Oma-az2 prod VCB-az2 prod	These Servers are the collection devices for VAM Data.	Patient demographic information, Patient healthcare information, lab orders/results, radiology orders/results, pharmacy order/results, procedures, clinical notes, vitals, allergies, problems, clinical user data, ordering clinician. All data that can pass into and out of the CPRS application passes from the client to the target.	Amazon Kinesis – Data Streaming Service

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

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

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

Follow the format below:

Privacy Risk: VAM has been categorized in the EPMO System Security Categorization as a High impact system based on the sensitive and important nature of the VistA data traffic that the VAM application monitors. The inherent risk from the VAM application is VistA traffic interruption. This can cause delays in day-to-day functions from providers.

Mitigation: However, the risk of information exposure is based on the VAEC security maintaining integrity. Cloud Service Provider (CSP) will not be affected by intentional or unintentional disclosure of PII, but VA will be affected. This solution supports VISTA data, and any disclosure of data will have a harmful effect on the VA and the magnitude will be same as VISTA data being disclosed. Because all information sharing is done within the VA network, per VA 6500 and 6510 requirements. Contractors working on the VAM Project are required to have PIV cards, Government Furnished Equipment (GFE - Laptops), VPN access to VA network and VA enterprise emails. Additionally, VAM RPCs only resides in the VAEC environment and have no external connections and VAM RPCs are not an End User based software, as well as there is no GUI (Graphical User Interface).

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?

VAM application has no external connection outside of VA. Information sharing only occurs within the VA Network.

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

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

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

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

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a

Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

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

Data Shared with External Organizations

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

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: High

Mitigation: VAM has been categorized in the EPMO System Security Categorization as a High impact system based on the sensitive and important nature of the VistA data traffic that the VAM application monitors. The inherent risk from the VAM application is VistA traffic interruption.

This can cause delays in day-to-day functions from providers. However, the risk of information exposure is based on the VAEC security maintaining integrity.

VAM application has no external connection outside of VAEC environment. VistA data is protected in the VAEC environment. All information sharing is done within the VA network, per VA 6500 requirements. Contractors working on the VAM Project are required to have PIV cards, Government Furnished Equipment (GFE - Laptops), VPN access to VA network and VA enterprise emails.

Section 6. Notice

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

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

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

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

The source information is VISTA data. Patients are provided with the The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
Which 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."

The VAM application has no external connections outside the VAEC. VAM Application / RPCs are not an End User based software. Moreover, there is no GUI (Graphical User Interface).

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

The VAM application has no external connections outside the VAEC. VAM Application / RPCs are not an End User based software. Moreover, there is no GUI (Graphical User Interface).
Notice was provided in accordance with 6.1a

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

Please provide response here

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.

The VAM application has no external connections outside the VAEC. VAM Application / RPCs are not an End User based software. Moreover, there is no GUI (Graphical User Interface).

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.

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.

N/A. The VAM application has no external connections outside the VAEC. VAM Application / RPCs are not an End User based software. Moreover, there is no GUI (Graphical User Interface).

Source 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. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: Has sufficient notice been provided to the individual?

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

Privacy Risk: VAM has been categorized in the EPMO System Security Categorization as a High impact system based on the sensitive and important nature of the VistA data traffic that the VAM application monitors. The inherent risk from the VAM application is VistA traffic interruption. This can cause delays in day-to-day functions from providers. However, the risk of information exposure is based on the VAEC security maintaining integrity

Mitigation: The VAM application has no external connections outside the VAEC. VAM RPCs are not an End User based software. Moreover, there is no GUI (Graphical User Interface). CSP will not be affected by intentional or unintentional disclosure of PII, but VA will be affected. This solution supports VISTA data, and any disclosure of data will have a harmful effect on the VA and the magnitude will be same as VISTA data being disclosed.

VAM is hosted in the VAEC environment and at High Assessing. System notices is a requirement inherited from the VA Enterprise as identified in the Customer Responsibility Matrix (CRM) attached under the evidence tab.

Section 7. Access, Redress, and Correction

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

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

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

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

The VAM application has no external connections outside the VAEC. VAM Application / RPCs is not an End User based software. Moreover, there is no GUI (Graphical User Interface).
The information is not maintained in a privacy act system of records however access is provided to the source documents in accordance with applicable SORNS and the Notice of Privacy Practices.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

N/A. The VAM application has no external connections outside the VAEC. VAM Application / RPCs is not an End User based software. Moreover, there is no GUI (Graphical User Interface). Information is not retrieved from the system by a personal identifier and is not covered by 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.

N/A. The VAM application has no external connections outside the VAEC. VAM Application / RPCs is not an End User based software. Moreover, there is no GUI (Graphical User Interface).

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.

N/A. The VAM application has no external connections outside the VAEC. VAM Application / RPCs is not an End User based software. Moreover, there is no GUI (Graphical User Interface).

Source documents can be corrected in accordance with the applicable SORNS and the notice of privacy practices.

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.

N/A. The VAM application has no external connections outside the VAEC. VAM Application / RPCs is not an End User based software. Moreover, there is no GUI (Graphical User Interface).

Source documents can be corrected in accordance with the applicable SORNS and the notice of privacy practices

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

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

N/A. The VAM application has no external connections outside the VAEC. VAM Application / RPCs is not an End User based software. Moreover, there is no GUI (Graphical User Interface).

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: VAM has been categorized in the EPMO System Security Categorization as a High impact system based on the sensitive and important nature of the VistA data traffic that the VAM application monitors. The inherent risk from the VAM application is VistA traffic interruption. This can cause delays in day-to-day functions from providers. However, the risk of information exposure is based on the VAEC security maintaining integrity.

Mitigation: The VAM application has no external connections outside the VAEC. VAM Application / RPCs is not an End User based software. Moreover, there is no GUI (Graphical User Interface). VA will be affected by intentional or unintentional disclosure of PII. This solution supports VISTA data, and any disclosure of data will have a harmful effect on the VA and the magnitude will be same as VISTA data being disclosed.

VAM provides security monitoring for all remote access clients (CPRS, JLV, CAPRI, …) of all veterans' health and benefits information in the Veterans Information System and Technology Architecture (VISTA) systems. The resulting issue from system failure is traffic interruption. Issue can be addressed through rescaling.

Section 8. Technical Access and Security

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

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

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

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

Access Request Process: 1. Identification of Need: The process begins when an individual within the organization identifies the need for access to the VAM system. This could be a healthcare professional, an IT staff member, a contractor, or any other authorized personnel who require access for their roles and responsibilities. 2.Access Authorization: The individual's supervisor or manager reviews the access request and determines whether the requested access is necessary for the individual to perform their job duties effectively. They consider the principle of least privilege, ensuring that the access granted aligns with the individual's job responsibilities and the principle of minimizing access to only what is essential. 3. Access Request Submission: Once the access authorization is granted by the supervisor or manager, the individual initiates an access request. This request typically goes through an electronic system, or an established process designated by the organization's IT department. 4. Access Request Form: The individual fills out an access request form that includes their personal information, job title, department, the specific components, or

functions within the VAM system they need access to, and the level of access required (read-only, edit, administrative, etc.). 5. Data Verification: The information provided in the access request form is verified by relevant authorities, such as the IT department, security team, or access control administrators. This verification helps ensure that the access request is legitimate and aligns with the individual's role and responsibilities. 6. Manager Approval: The access request form may require approval from the individual's supervisor or manager as an additional layer of authorization. The manager reviews the access request to ensure it is consistent with the individual's job requirements and approves or denies the request accordingly. 7. Access Provisioning: Once the access request is approved and verified, the IT department or access control administrators provision the necessary access rights to the VAM system. This involves configuring the individual's account settings and permissions according to the approved access request. 8. Account Activation: The individual is notified that their access has been provisioned and is now active. They receive login credentials, such as a username and password, along with any necessary instructions on how to access the VAM system. 9. Initial Login and Training: The individual logs in to the VAM system using the provided credentials. Depending on the sensitivity of the data and the complexity of the system, they may be required to undergo training on system usage, security practices, and privacy guidelines before they start using the system. 10. Ongoing Monitoring: Once access is granted, the individual's activities within the VAM system are monitored and audited to ensure compliance with security and privacy policies. Any unusual or unauthorized activities are flagged for investigation. The process described above ensures that individuals who require access to the VAM system go through a well-defined and controlled procedure. This process helps maintain the security of the system, prevents unauthorized access, and ensures that access is granted only to those who genuinely need it to fulfill their job responsibilities.

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?

The VAM (VistA Adaptive Maintenance) system is primarily designed for internal use within the VA (Department of Veterans Affairs) environment. Access to the system is typically limited to individuals, contractors, and authorized personnel within the VA who have specific job roles and responsibilities related to the system's operation, maintenance, and security. As a result, access by users from other external agencies is generally not a common scenario.

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.

Here is a description of the different roles created to provide access to the VAM (VistA Adaptive Maintenance) system, including their general permissions and responsibilities:

Administrator:

- This role has full control over the system.
- Can configure system settings, manage user accounts, and assign roles.
- Can grant and revoke permissions for all other roles.
- Responsible for maintaining system integrity and security.

System Operator:

- Monitors the system's health and performance.
- Manages system resources and troubleshoots technical issues.

- Can view system logs and perform diagnostics.
- Focuses on ensuring the system's smooth operation.

Analyst or Auditor:

- Reviews system logs and data for security and compliance.
- Has read-only access to logs and data for monitoring.
- Identifies unusual activities and potential security breaches.
- Ensures adherence to security policies.

Developer or Engineer:

- Has access to the system's codebase and configuration.
- Develops, implements, and maintains system updates.
- Troubleshoots and resolves technical issues.
- Responsible for system enhancements and improvements.

User Support Representative:

- Assists users with technical issues and inquiries.
- Can reset passwords and provide guidance on system usage.
- Helps users navigate the system and resolve minor issues.

Data Entry Operator:

- Enters and updates data in the system.
- Can create new records and modify existing information.
- Ensures data accuracy and completeness.
- Follows data entry protocols and guidelines.

Read-Only User:

- Has access to view data but cannot make changes.
- Generates reports and retrieves information from the system.
- Cannot modify or delete records.
- Focuses on data retrieval and analysis.

Manager or Supervisor:

- Oversees the work of other users.
- Reviews and approves data changes or requests.
- Manages access permissions for their team.
- Monitors system usage and compliance.

Security Officer:

- Enforces security policies and procedures.
- Reviews and manages access permissions.
- Conducts security assessments and identifies vulnerabilities.
- Addresses security incidents and ensures data protection.

Privacy Officer:

- Ensures compliance with privacy regulations and policies.
- Reviews data sharing agreements and PII handling practices.
- Addresses privacy concerns and inquiries.
- Focuses on protecting sensitive information.

External Collaborator:

- Given to users from external agencies or partners.
- Access is limited to specific tasks and data related to collaboration.
- Can interact with shared data and contribute to collaborative efforts.

These roles are designed to provide appropriate levels of access based on users' responsibilities and job functions. The permissions granted to each role are determined by system administrators and are

aligned with data security, privacy, and organizational needs. This role-based access control ensures that users can perform their tasks efficiently while maintaining the confidentiality, integrity, and availability of the system's data.

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.

Yes. VA Contractor access is verified through VA personnel before access is granted to any VA contractor. Contracts and contractor access are reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access.

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.

VAM Application is not an End User software. However, VA Contractors take and review TMS training, NDA (Non-disclosure agreement) Rules of Behavior, Security Awareness, per the VA 6500 and 6510.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Complete
2. *The System Security Plan Status Date:* 21 October 2020
3. *The Authorization Status:* Complete
4. *The Authorization Date:* 25 November 2019

5. *The Authorization Termination Date:* 5 November 2023
6. *The Risk Review Completion Date:* Complete
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Please provide response here

Section 9 – Technology Usage

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

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

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

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

Yes, the VAM (VistA Adaptive Maintenance) system utilizes cloud technology. Specifically, it is hosted within the VAEC (VA Enterprise Cloud) environment and utilizes Amazon Web Services (AWS) cloud services. The cloud model being utilized is the Infrastructure as a Service (IaaS) model. This means that the system leverages virtualized computing resources, storage, and networking provided by AWS to host and manage its infrastructure components, such as the RPC Monitor, RPC Mirror, and other architectural elements mentioned in the document. This cloud-based approach allows for scalability, flexibility, and efficient resource utilization. The VAM system operates within the VAEC GovCloud with a FedRAMP authorization granted on 25 Nov 2019. Cloud model is s PaaS.

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

NA

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.

NA

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.

NA

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).

NA

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

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

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2023.08.30 09:57:18 -04'00'

Privacy Officer, Nancy Katz-Johnson

Albertino M. Estacio 119921

Digitally signed by Albertino M. Estacio 119921
Date: 2023.09.01 08:55:20 -07'00'

Information System Security Officer, Albert Estacio

DAVID CATANOSO

Digitally signed by DAVID CATANOSO
Date: 2023.09.07 12:22:19 -04'00'

Information System Owner, David Catanoso

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).

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices