Privacy Impact Assessment for the VA IT System called:

VAEC Mobile Application Platform (Cloud) Assessing

Veterans Health Administration

VA Office of Information & Technology

Date PIA submitted for review:

6/2/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842-2000
Information System Owner	Daryl Kling	Daryl.Kling@va.gov	520-249-7190

Abstract

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

The VAEC Mobile Application Platform (MAP) is a cloud hosted system that provides the infrastructure and hosting platform for Mobile Shared Services (i.e. common services used for Mobile applications) and web components of applications used on Mobile devices. Mobile applications connect to VA enterprise services using the VAEC MAP Mobile Shared Services. Mobile applications such as Video Visits Service (VVS), Veteran Affairs Online Scheduling (VAOS), Patient Viewer (PV), and Veteran Affairs Video Connect (VVC) leverage this platform, pipeline, and hosting environment to provide a coordinated scheduling and notification capability to Staff and Veterans among other resources. Within the VAEC-MAP Security boundary are two environments: Production and Staging. Production provides the FISMA High environment that hosts the staff and veteran applications. This environment is integrated with several production VA systems for data sharing and authentication services that allow for single sign on within hosted applications. Staging provides the test ground for these applications to go through verification and validation (V&V) and integration testing with other VA test systems. This environment is maintained at a FIS MA Low categorization and has no direct connectivity to the production environment.

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.*

VAEC Mobile Application Platform (Cloud) Assessing VAEC Amazon

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

The VAEC Mobile Application Platform (MAP) is a cloud hosted system that provides the infrastructure and hosting platform for Mobile Shared Services (i.e. common services used for Mobile applications) and web components of applications used on Mobile devices. Mobile applications connect to VA enterprise services using the VAEC MAP Mobile Shared Services. Mobile applications such as Video Visits Service (VVS), Vete ran Affairs Online Scheduling (VAOS), Patient Viewer (PV), and Veteran Affairs Video Connect (VVC) leverage this platform, pipeline, and hosting environment to provide a coordinated scheduling and notification capability to Staff and Veterans among other resources. Within the VAEC-MAP Security boundary are two environments: Production and Staging. Production provides the FISMA High environment that hosts the staff and veteran applications. This environment is integrated with several production VA systems fo r data sharing and authentication services that allow for single sign on within hosted applications.

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

VAEC Amazon owned / VA controlled

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.*

Any Veteran or user of the system can have their info pulled into the databases for use with in the system supported by MAP. Guessing 25 -50k

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

The purpose of use will include, but not be limited to, health care treatment information, disability adjudication, and benefits to the Veteran both within the VA Medical Center and insharing with partners who are participating through the eHealth Exchange in VA's Mobile pilots and subsequent public and enterprise rollout of new applications. Data may also be used at an aggregate, non-personally identifiable level to track and evaluate local or national health and benefits initiatives and preventative-care measures, such as detecting outbreaks of flu or other diseases, detection of antibiotic resistance bacteria, etc.

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

While VAEC-MAP transmits information via Amazon Web Services (AWS) we do not share information in identifiable form or Personally Identifiable Information (PII) with any external (Outside of VA) organization, IT system, third-party website or application.

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.

The VA Dedicated Cloud is operated by Amazon Web Services (AWS) and uses a private cloud deployment model. The VA Dedicated Cloud is an Infrastructure as a Service (IaaS) cloud-computing platform.

3. Legal Authority and SORN

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

- 5 U.S.C. 552, "Freedom of Information Act," c. 1967
- 5 U.S.C. 552a, "Privacy Act," c. 1974
- 18 U.S.C. 1030 (a) (3), "Fraud and related activity in connection with computers."
- 38 U.S.C. 218, "Security and law enforcement on property under the jurisdiction of the Veterans Administration"
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems

- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- Executive Order 13103, Computer Software Piracy
- System of Record Notice (SORN) 73VA005OP2, "VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP)", https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf. Authority for Maintenance of the system: Title 38, United States Code, Section 501.
- VAEC-MAP collects processes and retains information from Veterans or dependents, VA employees, and VA contractors. Social Security Numbers (SSNs) are collected and used for secondary identification to the Electronic Data Interchange Personal Identifier (EDIPI) system. The legal authority to use or collect SSNs is Executive Order 9397

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?*
SORN for the system covers cloud usage.

D. System Changes

J. *Whether the completion of this PIA will result in circumstances that require changes to business processes*
The completion of this PIA will Not result in circumstances that require changes to business processes.

K. *Whether the completion of this PIA could potentially result in technology changes*
The completion of this PIA will not result in technology changes.

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
☒ Biometrics
☒ DD-214
☒ Claims Decision
☒ Other Data Elements (list below)

Health Information
Military Service Information
Patient ID
Integration Control Number (ICN)

PII Mapping of Components (Servers/Database)

VAEC-MAP consists of **19** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VAEC-MAP and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Admin	**Yes**	**Yes**	**Name, Address, Social Security**	**Provides staff and veterans**	**Encryption- in transit, at**

			Number, Phone Number	mobile access to information for veterans	rest and firewall ACLs
Bpr	Yes	Yes	Name, Address, Social Security Number, Phone Number	Provides staff and veterans mobile access to information for veterans	Encryption-in transit, at rest and firewall ACLs
Cloudconf	Yes	Yes	Name, Address, Social Security Number, Phone Number	Provides staff and veterans mobile access to information for veterans	Encryption-in transit, at rest and firewall ACLs
Courier	Yes	Yes	Name, Address, Social Security Number, Phone Number	Provides staff and veterans mobile access to information for veterans	Encryption-in transit, at rest and firewall ACLs
Facility-Definition	Yes	Yes	Name, Address, Social Security Number, Phone Number	Provides staff and veterans mobile access to information for veterans	Encryption-in transit, at rest and firewall ACLs
Local	Yes	Yes	Name, Address, Social Security Number, Phone Number	Provides staff and veterans mobile access to information for veterans	Encryption-in transit, at rest and firewall ACLs
Mongo-distributed-lock Note-writer	Yes	Yes	Name, Address, Social Security Number, Phone Number	Provides staff and veterans mobile access to information for veterans	Encryption-in transit, at rest and firewall ACLs
Orders	Yes	Yes	Name, Address, Social Security Number, Phone Number	Provides staff and veterans mobile access to	Encryption-in transit, at rest and firewall ACLs

				information for veterans	
Pagination	Yes	Yes	Name, Address, Social Security Number, Phone Number	Provides staff and veterans mobile access to information for veterans	Encryption-in transit, at rest and firewall ACLs
Patient-Search	Yes	Yes	Name, Address, Social Security Number, Phone Number	Provides staff and veterans mobile access to information for veterans	Encryption-in transit, at rest and firewall ACLs
Patient-Context	Yes	Yes	Name, Address, Social Security Number, Phone Number	Provides staff and veterans mobile access to information for veterans	Encryption-in transit, at rest and firewall ACLs
SV	Yes	Yes	Name, Address, Social Security Number, Phone Number	Provides staff and veterans mobile access to information for veterans	Encryption-in transit, at rest and firewall ACLs
Tasklist	Yes	Yes	Name, Address, Social Security Number, Phone Number	Provides staff and veterans mobile access to information for veterans	Encryption-in transit, at rest and firewall ACLs
Hadb	Yes	Yes	Name, Address, Social Security Number, Phone Number	Provides staff and veterans mobile access to information for veterans	Encryption-in transit, at rest and firewall ACLs
Mae_db	Yes	Yes	Name, Address, Social Security Number, Phone Number	Provides staff and veterans mobile access to information for veterans	Encryption-in transit, at rest and firewall ACLs

ConnectedHealth_db	**Yes**	**Yes**	**Name, Address, Social Security Number, Phone Number**	**Provides staff and veterans mobile access to information for veterans**	**Encryption-in transit, at rest and firewall ACLs**
CDW CDWWork	**Yes**	**Yes**	**Name, SSN, Date of birth, email, health information, benefits information, claims decision, DD-214, mailing address, phone number, biometrics**	**Provides staff and veterans mobile access to information for veterans**	**Encryption-in transit, at rest and firewall ACLs**
CDWWork2 (Millennium Cerner Data)	**Yes**	**Yes**	**Name, SSN, Date of birth, Race/ethnicity, Vital Status, Gender, City of residence, County of residence, Zip code, Hospitalization dates, Date of diagnosis, Date of death, Private insurance status, Laboratory results, Medications and therapies, Outpatient/inpatient clinic visits**	**Provides staff and veterans mobile access to information for veterans**	**Encryption-in transit, at rest and firewall ACLs**
Vista Imaging	**Yes**	**Yes**	**Name, address, SSN, DOB, Physician name, All data in DICOM**	**Provides staff and veterans mobile access to information for veterans**	**Encryption-in transit, at rest and firewall ACLs**

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?

Information is collected directly from individuals
The Digital Imaging and Communications in Medicine (DICOM) standard is used for transmitting patient image data for which the data elements listed in Section 1.1 are part of the Digital DICOM Header standard. The data elements are not collected separately as part of the Image Viewing Solution (IVS) Stroke Artificial Intelligence (AI) Operations.

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 Patients' image data is being used for the Image Viewing Solution (IVS) Stroke Artificial Intelligence (AI) Operations. Each image study has patient PII metadata attached as a part of the Image DICOM Header

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

Image Viewing Solution (IVS) Stroke Artificial Intelligence (AI) Operations analyzes the patients' images and creates an AI image analysis Image Series and Report for each patient case processed through the Nicolab HALO Stroke AI Image Analysis algorithm(s)

1.3 How is the information collected?

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

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

VA staff or veteran information is solicited through mobile applications hosted in and accessed by the VAEC-MAP. This information is accessed through mobile applications and aggregated from inter-connected VA systems. This provides staff and veterans mobile access to information for veterans in pre-production/production environment
Patient Image PII metadata is provided to the Image Viewing Solution (IVS) Stroke Artificial Intelligence (AI) Operations system from the DICOM Header and is reused for the labeling the AI created Image series and the Stroke AI created report.

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.

No, there is no paperwork with the system.

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

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

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

The system writes the data to both the primary and to the secondary area at the same time. In doing this, the data remains completely current and identical. The process works quickly and there is an extremely small margin of error. Because of this, it is ideal for disaster recovery and is the method preferred for projects that require absolutely no data loss.
Patient information is not stored in the Image Viewing Solution (IVS) Stroke Artificial Intelligence (AI) Radiology Image Analysis internal VA IT system. There are no computer matching agreements in place with another government agency. The Digital Imaging and Communications in Medicine (DICOM) commands (e.g., C-Store, C-Find, C-Get, etc.) and the DICOM Protocols checks for data accuracy each time the DICOM commands are executed.

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

N/A system only talks to internal VA systems and DHA.

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

- 5 U.S.C. 552, "Freedom of Information Act," c. 1967
- 5 U.S.C. 552a, "Privacy Act," c. 1974
- 18 U.S.C. 1030 (a) (3), "Fraud and related activity in connection with computers."
- 38 U.S.C. 218, "Security and law enforcement on property under the jurisdiction of the Veterans Administration"
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems
- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- Executive Order 13103, Computer Software Piracy
- VAEC-MAP collects processes and retains information from Veterans or dependents, VA employees, and VA contractors. Social Security Numbers (SSNs) are collected and used for secondary identification to the Electronic Data Interchange Personal Identifier (EDIPI) system. The legal authority to use or collect SSNs is Executive Order 9397
- System of Record Notice (SORN) 73VA005OP2, "VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP)", https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf. Authority for Maintenance of the system: Title 38, United States Code, Section 501.

Image Viewing Solution (IVS) has two (2) Food and Drug Administration (FDA) 510K approved medical devices (ResolutionMD and Nicolab HALO). These medical devices have Class II certifications from the FDA for which is accepted by the Department of Veterans Affairs to operate in the VA environment under VA directive 6550, PRE-PROCUREMENT ASSESSMENT AND IMPLEMENTATION OF MEDICALDEVICES/SYSTEMS

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

<u>Privacy Risk:</u> There is a risk that sensitive information could be incorrectly handled.

<u>Mitigation:</u> VAEC-MAP adheres to information security requirements instituted by the VA Office of Information Technology (OIT). VAEC-MAP implements cryptography that is compliant with federal laws and regulations i.e., FIPS 140-2. Any deviation from Federal requirements will be documented in a Risk-Based Decision Memo and approved as a long-term managed risk by VA management.

VA employees and contractors with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually

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.

Name – Used to correctly identify the mobile application user.

Mailing Address – Used to correctly identify user

Social Security Number – Used to correctly identify user

Phone Number – Used to correctly identify user

Health Information – Used to correctly identify user and patient care

Financial Information – Used to correctly identify user

Email Address – Used to correctly identify user

Military Service Information – Used to correctly identify user and patient care

Biometrics – Used to correctly identify user and patient care

DD-214-Used to correctly identify user and patient care

Claims Decision - patient care

The Image Viewing Solution (IVS) Stroke Artificial Intelligence (AI) Radiology Image Analysis system does not use information external to the VA. The Image Viewing Solution (IVS) Stroke Artificial Intelligence (AI) Radiology Image Analysis system uses information for the VA National Telestroke Program (NTSP) clinical evaluations of Acute Stroke Victims

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.

Information collected is utilized by Authentication and Authorization services of Active Directory and mobile applications in the production application environment.
There is some analytics done but this is done on the OCC application/data team level not by the infrastructure team. The CCP team makes sure that there is connectivity for the systems to communicate.
The Image Viewing Solution (IV) Stroke Artificial Intelligence (AI) The Stoke AI Image Analysis AI Image Series and an AI Image Analysis Report are stored in the Acuo VNA with the Patient's original CT or CTA scans and are available to the Telestroke medical providers to review and analyze, through use of the IVS. These newly created medical artifacts assist the Telestroke Neurologist with rapid stroke diagnosis and treatment plans for the patients

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.

The Image Viewing Solution (IV) Stroke Artificial Intelligence (AI) Algorithms performs Radiology (CT and CTA scans) image analysis to identify stroke pathology in the scans. The Stoke AI Image Analysis Algorithms creates an AI Image Series and an AI Image Analysis Report and both artifacts are labeled with patient PII metadata for patient PHI identification

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?

VA has processes to protect information at rest, in storage, or in transit that include but are not limited to:

- VA approved encryption such as FIPS 140-3 or current version
  - Full disk encryption (FDE)
  - Virtual disk and volume encryption and
  - File/folder encryption

- Intrusion Detection and Protection Systems (IDPS)
- Firewalls rulesets
- Endpoint security to scan for malware other threats to confidentiality and integrity.
- Physical and logical access control Mechanisms
- Change control process

SSL encrypted TCP sessions to the data sources

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

SSL encrypted TCP sessions to the data sources

The Stroke Artificial Intelligence (AI) information is encrypted in transit and at rest and uses Transport Layer Security (TLS) as well.

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

Access to and use of national administrative databases, warehouses, and data marts are limited to those persons whose official duties require such access, and VA has established security procedures to ensure that access is appropriately limited. Information security officers and system data stewards review and authorize data access requests. VA regulates data access with security software that authenticates users and requires individually-unique codes and passwords. VA requires information security raining for all staff and instructs staff on the responsibility each person has for safeguarding data confidentiality. Physical access to computer rooms housing national administrative databases, warehouses, and data marts is restricted to authorized staff and protected by a variety of security devices.

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:

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

<u>Principle of Use Limitation:</u> 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?

Individual users are given access to Veteran's data through the issuance of ePAS and ISO approval, and by the use of a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication.
Access to the Image Viewing Solution (IVS)/ IVS Stroke Artificial Intelligence (AI) Operations is limited to medical staff that have credentials to access VistA/CPRS.

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

All employees and contractors with access to Veteran's information are required to complete the VA Privacy and Information Security awareness training and rules of behavior annually. The VA Talent Management System (TMS) tracks, monitors, and records all employee and contractor training. Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.

2.4c Does access require manager approval?

Yes, manager approval is needed to get PIV access, Roles are assigned designating who has access to what data.

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

VAEC MAP provides individuals the right of access, under the Privacy Act of 1974, only to their records which are not exempt pursuant to subsections (j) and (k) of the Privacy Act.» Access is given only to information which is retrieved by the individual's own personal identifier(s).» The VAEC MAP Release of Information department processes medical records requests for veterans, third and first parties.» The VA Form 10-5345 is used for the Veteran to authorize disclosure to third parties.» The Privacy Officer conducts monitors of the Release of Information, which is reported to VA Privacy Compliance Assurance team quarterly.» Veterans may obtain medical records with a written request or on VA Form 10-5345a.» Veterans may also view their medical records on My HealtheVet, after signing up.» If required, each VAEC MAP SORN contains "Notification" and "Access" sections that indicate the official to whom such requests should be directed.» An individual wanting notification or access, including contesting the record, should mail or deliver a request to the office identified in the SORN. If an individual does not know the “office concerned,” the request may be addressed to the PO or FOIA/PO of any VA field station or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420.» VAEC MAP provides a First party right of access to records contained in the Privacy Act SOR (System of Record).» Police Reports (UORs) are requested via Freedom of Information Act (FOIA); however, other records are requested in writing through the Privacy Officer.» Access to any non-medical record will be directed to the Privacy Officer.» Requests to review medical records in their original form will be processed by the Privacy Officer.

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

VAEC Privacy officer is responsible for assuring safeguards for 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*

- Name
- Mailing Address
- Social Security Number
- Phone Number
- Health Information
- Financial Information
- Email Address
- Military Service Information
- Biometrics
- DD-214
- Claims decisions

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.*

• Retains PII (name and account information) for the minimum amount of time to fulfill the systems purpose or as required by law;
• Dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage in accordance with a NARA-approved record retention schedule and in a manner, that prevents loss, theft, misuse, or unauthorized access; and
• Use approved records disposition schedules to ensure secure deletion or destruction of PII (including originals, copies, and archived records).
• VAEC-MAP follows the requirements of a FISMA High system and retains information for 6 years. Records from this system that are needed for audit purposes will be disposed of 6 years after a user's account becomes inactive.

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

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

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

Yes, NARA requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization.

All systems with a FISMA High rating have the same Data Retention requirements that have been approved by the VA and would be recorded under the VAEC GSS – Assessing ATO package.

Routine records will be disposed of when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes. These retention and disposal statements are pursuant to NARA General Records Schedules GRS 3.2, item 030 and item 031. (https://www.archives.gov/files/records-mgmt/grs/grs03-2.pdf).

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

NARA General Records Schedules GRS 3.2, item 030 and item 031.
(https://www.archives.gov/files/records-mgmt/grs/grs03-2.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.

Dissemination procedures fall under AWS, as determined in the contract between AWS and VA. Since all information is located on the Cloud (AWS) there are no tangible documents to discard.

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.

VAEC-MAP adheres to information security requirements instituted by the VA Office of Information Technology (OIT). VAEC-MAP implements cryptography that is compliant with federal laws and regulations i.e., FIPS 140-2.

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. (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:

<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?

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: The information is necessary to accomplish the purpose of VAEC-MAP implementation. It's possible that VA account credentials may be released to unauthorized individuals.

Mitigation: VAEC-MAP implements cryptography that is compliant with federal laws and regulations, i.e., FIPS 140-2. Any deviation from Federal requirements will be documented in a Risk-Based Decision Memo and approved as a long-term managed risk by VA management. VA employees and contractors with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. VAEC-MAP follows GRS 3.2 30 and 31 and all information is disposed securely, as described in 3.4.

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***
Clinical Data System/Health Data Repository (CDS/HDR)	VAEC MAP connects to several other IT systems leveraging and storing information they provide for Mobile Applications to function correctly and serve both staff and veterans with information specific to the capabilities of those applications.	Information consists of health information, financial information, SSN, Address, e-mail address, and Military Service Information	SSL encrypted TCP sessions to the data sources
Member Services and Data Information (MSDI)	VAEC MAP connects to several other IT systems leveraging and storing information they provide for Mobile Applications to function correctly and serve both staff and veterans with information specific to the capabilities of those applications.	Information consists of health information, financial information, SSN, Address, e-mail address, and Military Service Information	SSL encrypted TCP sessions to the data sources
My HealtheVet (MHV)	VAEC MAP connects to several other IT systems leveraging and storing	Information consists of health information, financial information, SSN, Address, e-mail address, and Military Service Information	SSL encrypted TCP sessions to the data sources

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*
	information they provide for Mobile Applications to function correctly and serve both staff and veterans with information specific to the capabilities of those applications.		
Corporate Data Warehouse (CDW)	VAEC MAP connects to several other IT systems leveraging and storing information they provide for Mobile Applications to function correctly and serve both staff and veterans with information specific to the capabilities of those applications.	Information consists of health information, financial information, SSN, Address, e-mail address, and Military Service Information	SSL encrypted TCP sessions to the data sources
Master Veteran Index (MVI)	VAEC MAP connects to several other IT systems leveraging and storing information they provide for Mobile Applications to function correctly and serve both staff and veterans with information specific to	Information consists of health information, financial information, SSN, Address, e-mail address, and Military Service Information	SSL encrypted TCP sessions to the data sources

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*
	the capabilities of those applications.		
VAEC MAP ISA Single Sign on External (SSOe)	Used for Authentication	Information consists of health information, financial information, SSN, Address, e-mail address, and Military Service Information	SSL encrypted TCP sessions to the data sources
Veteran Affairs DSLogon	Used for Authentication	Login information used by Veterans to access patient facing applications	Proxied by IAM

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The information is necessary to accomplish the purpose of VAEC-MAP implementation. It's possible that VA account credentials may be released to unauthorized individuals.

Mitigation: VAEC-MAP implements cryptography that is compliant with federal laws and regulations, i.e., FIPS 140-2. Any deviation from Federal requirements will be documented in a Risk-Based Decision Memo and approved as a long-term managed risk by VA management. VA employees and contractors with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. VAEC-MAP follows GRC 20 and 24 and all information is disposed securely, as described in 3.4.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

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: VAEC-MAP does not share information in identifiable form or Personally Identifiable Information (PII) with any external (Outside of VA) organization, IT system, third-party website or application.

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 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.

Notice has been provided prior to the collection of the information in the following ways:

PRIVACY ACT STATEMENT: Use of VA Licensed Software by you may involve the collection of individually identifiable data that you enter into the Application and data about your use of the Application. As authorized by 38 U.S.C. Section 501, VA is asking you to provide information via this Application which may be included with other information VA uses to deliver health care to you. VA may disclose the information that you entered into the Application as permitted by law. VA may make a "routine use" disclosure of the information as outlined in the Privacy Act systems of records notices and in accordance with the Veterans Health Administration (VHA) Notice of Privacy Practices. VHA will explain these routine uses and privacy practices upon further request. Providing the information is voluntary. Failure to furnish your identifying information (username and login) when required by an application will prevent you from being able to use the Licensed Software, but will not have any effect on any other benefits or care to which you may be entitled. VA may also use this information to identify users of the Licensed Software, and for other purposes authorized or required by law.

The SORN for this system is VA Enterprise Cloud – Mobile Application Platform (Cloud) Assessing (VAEC-MAP) is 173VA005OP2. https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf.

Veterans are informed of the amendment process by many resources to include the Notice of Privacy Practice (NOPP) https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946 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 or health records.
>
> If your request for amendment is denied, you will be notified of this decision in writing and given information about your right to appeal the decision. In response, you may do any of the following:
>
> - File an appeal.
> - File a “Statement of Disagreement” which will be included in your health record
> - Ask that your initial request for amendment accompany all future disclosures of the disputed health information.

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

Notice was provided. See response to 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.

The VA Notice of Privacy Practices (NOPP) is provided to Veterans when they enroll for treatment with at a Veterans Health Administration facility. Copies of the NOPP are mailed to Veterans any time the document is updated or every 3 years after it is published. Copies of the notice may also be obtained by contacting a VHA facility Privacy Officer. It may also be accessed by the public online on the VA Publication site or at this link: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946.

The SORN for this system, 173VA005P2 - VA Enterprise Cloud – Mobile Application Platform (Cloud) Assessing (VAEC-MAP) is available to the public online at this link: https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf.

This Privacy Impact Assessment may also serve as a notice as it will be published online where it is accessible to the public at https://www.oprm.va.gov/privacy/pia.aspx.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

VHA permits individuals to agree to the collection of their personally identifiable information (PII) through the use of 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 and conversations with VHA employees. VA Forms are reviewed by VHACO periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations were 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.

There is no penalty assessed if an individual chooses not to provide information. However, in doing so the individual may be limiting the amount of pertinent information needed to provide benefits or treatment.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent *is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.*

VHA permits individuals to agree to the collection of their personally identifiable information (PII) through the use of 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 and conversations with VHA employees. VA Forms are reviewed by VHACO periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations were 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 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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

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

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

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

<u>Privacy Risk:</u> There is a risk that an individual may not understand what their information is being collected or maintained about them.

<u>Mitigation:</u> This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries when there is a change in regulation. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notice (SORNs) and Privacy Impact Assessment (PIA) available for review online. Additionally, FIPS 199 high classification Standards for Security Categorization of Federal Information and Information Systems are applied to the VAEC-MAP environment.

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.***

There are several ways a veteran or other beneficiary may access information about them:

The Notice of Privacy Practice (NOPP), which every patient receives when they enroll, discusses the process for requesting an amendment to one's records.

The VHA staffs Release of Information (ROI) offices at facilities to assist Veterans with obtaining access to their health l records and other records containing personal information.

The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their health records. The Veteran must enroll to obtain access to all the available features.

In addition, VHA Directive 1605.01, Privacy and Release of Information, establishes procedures for Veterans to have their records amended where appropriate.

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 - This system is not exempt from individual right of access.

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 – This system is covered by SORN 173VA005P2.

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.

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SORN. Every Privacy Act SORN contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

Employees should contact their immediate supervisor and Human Resources to correct inaccurate or erroneous information. Contractors should contact Contract Officer Representative to correct inaccurate or erroneous information upon request.

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 by many resources to include the Notice of Privacy Practice (NOPP) https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946 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 or health records.

If your request for amendment is denied, you will be notified of this decision in writing and given information about your right to appeal the decision. In response, you may do any of the following:

- File an appeal.
- File a “Statement of Disagreement” which will be included in your health record
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information.

Information may also be obtained by contacting the VHA facility Release of Information office.

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 - there is a formal process in place.

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: There is a risk that a Veteran does not know how to obtain access to their records or how to request corrections to their records and that the health record could contain inaccurate information and subsequently effect the care the Veterans receive.

Mitigation: As discussed in question 7.3, the Notice of Privacy Practice (NOPP), which every patient receives when they enroll, discusses the process for requesting an amendment to one's records.

The VHA staffs Release of Information (ROI) offices at facilities to assist Veterans with obtaining access to their health l records and other records containing personal information.

The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their health records. The Veteran must enroll to obtain access to all the available features.

In addition, VHA Directive 1605.01, Privacy and Release of Information, establishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

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

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.

Authentication and authorization are used to determine access to all systems within VAEC-MAP VA Medical Providers/professionals, both VA employees and contractors, have access to the Image Viewing Solution (IVS) Stroke Artificial Intelligence (AI) Information through the IVS which is a Staff only system. IVS users Authenticate into the IVS system by using their VistA Computerized Patient Record System (CPRS) Access and Verify Codes. IVS users must complete VA security and Privacy training in order to get access to CPRS and therefore have completed the same VA security and Privacy training to gain access to the IVS.

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?

Image Viewing Solution (IVS) Stroke Artificial Intelligence (AI) Information system has only one role, which is Staff, and can only be accessed by VA staff members. The Digital Imaging and Communications in Medicine (DICOM) standard is used for transmitting patient image data for which the data elements listed in Section 1.1 are part of the Digital DICOM Header standard. The patients' PII data elements are shared as part of the image transmission using the DICOM Header standard within the Image Viewing Solution (IVS) Stroke Artificial Intelligence (AI) Operations.

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.

With in the VAEC console there are 3 roles Read-Only, Limited Admin and Full admin. The access is based off that the person is doing within the system.

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.

Contracts are reviewed annually by the Contracting Officer or Contracting Officer's Technical Representatives to ensure that security requirements and security specifications are explicitly included in the information systems and information system support service acquisition contracts. In addition, contracts contain the appropriate security language necessary for compliance with FISMA and 38 U.S.C 5721-28 and provide adequate security for information and information systems used by the contractor.
All VA contractors are required to sign a NDA prior to receiving access to the system and working on the project. Contractor involvement will include System Administration of the database servers that house the PII and PHI information.

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.

VA requires personnel who have access to VA PHI to complete additional annual privacy training specific to their responsibilities in handling VA PHI covered under Health Insurance Portability and Accountability Act (HIPAA). Specific training methods include, but are not limited to: -Mandatory annual privacy awareness training; -Targeted, role-based training; -Internal privacy program Web sites; -Manuals, guides, and handbooks; -Slide presentations; -Events (e.g., privacy awareness week, privacy clean-up day); -Posters and brochures; -Email messages to employees and contractors.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date: 9 NOV 2022*
3. *The Authorization Status:* ATO
4. *The Authorization Date:* 20 Jan 2023
5. *The Authorization Termination Date:* 19 Jul 2023
6. *The Risk Review Completion Date:* 4 Jan 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

N/A

Section 9 – Technology Usage

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

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

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

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

YES, Infrastructure as a Service (IaaS)/ VAEC No further responses required.

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.*

Please provide response here

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.

Please provide response here

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.

Please provide response here

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).

Please provide response here

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**

ID	Privacy Controls
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.

Phillip Cauthers 255139

Digitally signed by Phillip Cauthers 255139
Date: 2023.06.09 12:20:02 -07'00'

Privacy Officer, Phillip Cauthers

JAMES BORING

Digitally signed by JAMES BORING
Date: 2023.06.10 10:37:05 -04'00'

Information System Security Officer, James Boring

Daryl A. Kling 3602439

Digitally signed by Daryl A. Kling 3602439
Date: 2023.06.12 09:38:16 -07'00'

Information System Owner, Daryl Kling

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).

The SORN for this system is 173VA005OP2 "VA Enterprise Cloud – Mobile Application Platform (Cloud) Assessing (VAEC-MAP)": https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf.

Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

VHA Directive 1605.01, Privacy and Release of Information:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3233

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