Privacy Impact Assessment for the VA IT System called:

Calabrio Advanced Quality Monitoring (AQM)

Office of Information Technology (OI&T)

Connectivity and Collaboration Services (CCS)/Unified Communications (UC)

Date PIA submitted for review:

10.10.2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	tonya.facemire@va.gov	202-632-8423
Information System Security Officer (ISSO)	Chirag Patel	chirag.patel3@va.gov	610-384-7711 x4556
Information System Owner	Bradley Mills	Bradley.Mills@va.gov	(202) 632-9603

Abstract

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

Calabrio Advanced Quality Monitoring (AQM) is an Enterprise solution that will be located at the four Trust Internet Connection (TIC). Calabrio will provide Advance Quality Management (AQM), Workforce Management (WFM) and Analytics Solution. The AQM will be used to capture voice/screen recording and provide real time monitoring. The WFM will provide the ability to forecast staffing, and to manage agents scheduling. The Analytics solution shall have the ability monitor and review performance from the agent's and can support additional languages. The AQM, WFM and Analytics solution will integrate to the Cisco Unified Contact Center Enterprise (UCCE) and Cisco Unified Contact Center Express (UCCX) 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.*

Office of Information Technology, Connectivity and Collaboration Services (CCS), Unified Communications (UC).

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

The Department of Veterans Affairs (VA) and its administration offices (VHA, VBA and NCA) have need for an Enterprise Solution that will enhance the veteran needs for advance technology within a call center environment. This procurement for AQM, WFM and Analytics Solution will be used to improve customer satisfaction and manage performance. These improvements will help in providing a more positive and efficient experience for Veterans and their spouses.

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

VA Owned and VA Operated.

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.*

The build out of the system at this time is for 14K VA contact center agents. The information that will be stored will be the interaction of veteran's/spouse and the VA contact center agents.

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

The information will collect Names, Phone Numbers, Social Security Numbers, File Numbers, addresses, personal email, Date of Birth, Health Insurance number, medical record number, Tax ID and emergency contact information. The information will be collected as part of the call recordings and screen captures that the system will store in order to be used to improve customer satisfaction and manage call center agent performance.

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

There is no internal or external sharing by this system

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.*

PII/PHI will be maintained at TIC South and North utilizing media file standard storage (SQL server) utilizing encryption that meets FIPS 140-2 compliance.

3. Legal Authority and SORN

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Sections 501(b) and 304. Per SORN 24VA10A7/85 FR 62406, Patient Medical Records-VA. This system contains a Consolidated Health Record (CHR) for patients and includes identifying information such as Social Security Number, medical history, employment history, medical benefit and eligibility information, and patient admission and discharge information. https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38 United States Code 7301(a); Title 38 United States Code 1703— Veterans Community Care Program; Veterans Access, Choice, and Accountability Act of 2014 (Pub. L. 113–146). Per SORN 180VA10D/83 FR 64935, Health Share Referral Manager (HSRM)-VA. This system automatically generates referrals and authorizations for all Veterans receiving care in the VA community and contains information including identifying information such as Social Security Number, contact information, taxpayer identification, eligibility, and health care provider details. https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17527.pdf

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and title 38, U.S.C. §501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77. Title 5 U.S.C. 5514. Per SORN 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. This system contains records relating to the administration of claims of veterans, service members, reservists, their spouses, and dependents for a wide variety of Federal veteran's benefits. https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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?*

The system is not in the process of being modified.

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 the circumstances that require changes to the business processes.

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

The completion of this PIA could not potentially result in technology change.

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)

File Number

PII Mapping of Components (Servers/Database)

Calabrio AQM consists of 36 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 Calabrio AQM 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
VAPNSFONWO EAPA1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWO EAPA2/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit

VAPNSFONWO EAPA3/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWO EABA1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWO EAPB1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWO EAPB2/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWO EAPB3/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWO EABB1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWO EAPO1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWO EAPO2/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical	Quality Management and Coaching.	Encryption at Rest and In Transit

			record number		
VAPNSFONWO EAPO3/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWO EABO1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONW OEAPA1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONW OEAPA2/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONW OEAPA3/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONW OEABA1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONW OEAPB1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONW OEAPB2/ Calabrio VA	Yes	No	Name, address, phone, DOB,	Quality Management and Coaching.	Encryption at Rest and In Transit

			SSN, medical record number		
VAPNNFONW OEAPB3/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONW OEABB1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONW OEAPO1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONW OEAPO2/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONW OEAPO3/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONW OEABO1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONW OVAPB1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit

VAPNNFONW OVAPB2/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONW OVABB1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNEFONWO VAPC1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNEFONWO VAPC2/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNEFONWO VABC1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWO VAPA1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWO VAPA2/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWO VABA1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical	Quality Management and Coaching.	Encryption at Rest and In Transit

			record number		
VAPNWFONW OVAPD1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNWFONW OVAPD2/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNWFONW OVABD1/ Calabrio VA	Yes	No	Name, address, phone, DOB, SSN, medical record number	Quality Management and Coaching.	Encryption at Rest and In Transit

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

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

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

The sources of information will be provided by Veterans and/or their dependents/Caretakers.

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.

No information from sources other than the individuals will be required as the system only records and maintains information from Veterans and/or their dependents.

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

VA management will review the recording for evaluation purpose/improve the agent performance and to verify the accuracy of the information that is being given to the veteran/caretaker. Calabrio AQM analytics platform will transform every veteran's interaction into usable data for evaluation.

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?

Audio/Screen recording is collected by Calabrio-AQM. If (incoming/outgoing) calls are designated to utilize the VA call center, calls are then recorded per the business request. VA business practice would then come into play in using the recordings based on their requirements.

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.

The information is not collected on a form and is not subject to the Paperwork Reduction Act,

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

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

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

Information (recordings) will be check by a VA Quality Manager (QM) and VA Workforce Manager (WFM). The VA QM/WFM personal and VA agents will have the ability to evaluate/review the recordings which would allow both parties to the understand performance criteria of the work. Business units will dictate their requirements on how often they will review recordings for quality/evaluation purpose.

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

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Sections 501(b) and 304. Per SORN 24VA10A7/85 FR 62406, Patient Medical Records-VA. This system contains a Consolidated Health Record (CHR) for patients and includes identifying information such as Social Security Number, medical history, employment history, medical benefit and eligibility information, and patient admission and discharge information. https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38 United States Code 7301(a); Title 38 United States Code 1703— Veterans Community Care Program; Veterans Access, Choice, and Accountability Act of 2014 (Pub. L. 113–146). automatically generates referrals and authorizations for all Veterans receiving care in the VA community and contains information including identifying information such as Social Security Number, contact information, taxpayer identification, eligibility, and health care provider details. https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17527.pdf

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and title 38, U.S.C. §501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77. Title 5 U.S.C. 5514. Per SORN 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. This system contains records relating to the administration of claims of veterans, service members, reservists, their spouses, and dependents for a wide variety of Federal veteran's benefits. https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

Principle of Purpose Specification: 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: Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional or financial harm may result for the individuals affected.

Mitigation: The Calabrio AQM resides entirely within VA domain and firewalls, with a URL link to Microsoft Azure for archiving. The Calabrio AQM recording are encrypted and secured with the VA secure TIC sites. Access to authenticated caller is limited to one client record information, and only to specific field information regarding payment amount, payment date, and claim establishment date.

- Data is collected at the Veteran's consent as he/she provides the information.
- Veteran must authenticate self, using approved Office of General Counsel and VA security approved criteria.
- Only the minimal amount of data needed is used for authentication and response.
- Policies and procedures are in place to ensure that PII is accurate, complete and current.
- Inaccuracy or error will be immediately reported by Veteran with live agent during the call.

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 as a veteran identifier
Social Security Number	Used as a veteran identifier
Date of Birth	Used to identify veteran and age
Phone Number(s)	Used for communication
Financial Account Information	Confirms veteran's last benefit payment (VBA)
Veteran File Number	Used as an alternative veteran identifier
Status of Claim	Used as a veteran information
Medical History	Used as a veteran information

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.*

The system will not make or create unutilized information. The Calabrio AQM will not have the ability to alter any information that is being recorded. No recording will be placed in an individual's record.

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.

Every time the veteran/caretaker calls into the Contact Center a new recording will be created and archive. Only action that will be taken will be identifying the reason for the veteran/caretaker call. VA managers will have access to the recording. VA mangers will have the ability to allow the VA agent who took the call the ability to listen to the recording for evaluation purpose.

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?

Any VA owned PII/PHI that resides at rest on the system are encrypted with FIPS 140-2 Encryption compliance. The servers that retain the information also meet the VA baseline configurations to ensure operations of those servers, to include Vulnerability Management, are closely monitored each day.

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

The system is also monitored via internal auditing tools to include ICAMP and any misconfiguration or unapproved changes are reported directly to the system owner and assigned ISSO.

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

The system identifies personnel with significant information system security roles and responsibilities. (i.e., system managers, system administrators, contracting staff), documents those roles and responsibilities, and provides appropriate additional information system security training. Security training records will be monitored and maintained. Each system user must maintain compliance with their assigned security and privacy training, or their overall system access may be disabled until they are showing proof of compliance. Access controls are in place to ensure that users with a need to know in the course of their duties have been assigned correctly to access VA owned PII/PHI.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

Access to VA owned PII/PHI requires supervisor and/or designee approval before any access can be provided. Access is assigned based on the role/position of the individual employee which has been requested by their assigned supervisor and/or designee. Access control measures ensure that the individuals with access to PII/PHI are only granted access to those options that they have a need to know in the course of their assigned duties.

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

Access requirements and roles are documented within in accordance with VA Policy. Individuals granted access to PII/PHI adhere to the VA security and privacy listed within VA Handbook 6500 by utilizes approved access control methods such as Electronic Permission Access System (EPAS).

2.4c Does access require manager approval?

Access to VA owned PII/PHI requires supervisor and/or designee approval before any access can be provided.

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

The controls in place to assure that the information is handled in accordance with the uses described above include mandatory online information security and Privacy and HIPAA training; face-to-face training for all incoming new employees conducted by the Information System Security Officer and Privacy Officer; and regular audits of individuals accessing sensitive information.

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

The system owner is ultimately responsible for ensuring all security and privacy controls have been implemented. End User supervisors and/or designees are also responsible for ensuring that their employees have only the access they need to have in the course of their assigned duties to ensure their employees adhere to least privilege requirement.

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*

Calabrio AQM will be retaining audio/screen recording (SSN, name, DOB, address, medical record number, Health Insurance number, veteran file #). These recording will be the interaction between the VA agent and the veteran/caregiver as they fully engage with the VA agent.

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.*

Archive- VA policy dictates that records will be retained for seven (7) years.

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. All records that are stored within the system boundary are stored in accordance with VA Retention policies and guidelines.

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

Records Control Schedule VB–1, Part 1 Section XIII, Item 13–052.100;
Records Control Schedule (RCS), RCS VB–1, Part I, Field in Section VII, dated January 31, 2014;
VHA Records Control Schedule (RCS 10–1), Chapter 66000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3).
Record Control Schedule (RCS) 10–1 item; 2201.1. (GRS) 5.1 item 010, DAA–GRS–2017– 0003–0001rcs10-1.pdf (va.gov)

Per SORN 24VA10A7/85 FR 62406, Patient Medical Records-VA. This system contains a Consolidated Health Record (CHR) for patients and includes identifying information such as Social Security Number, medical history, employment history, medical benefit and eligibility information, and patient admission and discharge information. https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

Per SORN 180VA10D/83 FR 64935, Health Share Referral Manager (HSRM)-VA. This system automatically generates referrals and authorizations for all Veterans receiving care in the VA community and contains information including identifying information such as Social Security Number, contact information, taxpayer identification, eligibility, and health care provider details. https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17527.pdf

Per SORN 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. This system contains records relating to the administration of claims of veterans, service members, reservists, their spouses, and dependents for a wide variety of Federal veteran's benefits. https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.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.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.
https://www.va.gov/vapubs/search_action.cfm?dType=1"

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

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

The recording will not be used for testing and research. Training will only be used for quality and evaluation purpose by the QM/WFM manager and agent being reviewed. Calabrio AQM is FIPS-140-2 compliant. Access to the recordings requires two-factor-authentication and privileges are controlled by Access Control List (ACL).

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?

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

Follow the format below:

<u>Privacy Risk:</u> There is a risk that the information maintained by Calabrio AQM could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released, breached, or exploited for reasons other than what is described in the privacy documentation associated with the information.

<u>Mitigation:</u> To mitigate the risk posed by information retention, Calabrio AQM adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4. The Calabrio AQM system ensures that all personnel involved with the collection, use and retention of data are trained in the correct process for collecting, using and retaining this data. A Records Management Officer (RMO), Privacy Officer (PO) and an Information System Security Officer (ISSO) are assigned to the boundary to ensure their respective programs are understood and followed by all to protect sensitive information form the time it is captured by the VA until it is finally disposed of. Each of these in-depth programs have controls that overlap and are assessed annually to ensure requirements are being met and assist staff with questions concerning the proper handling of information.

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***
Information will not be shared	N/A	N/A	N/A

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:

<u>Privacy Risk:</u> There is no internal sharing or disclosure.

<u>Mitigation:</u> There is no internal sharing or disclosure.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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

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:

<u>Privacy Risk:</u> **There is no internal or external sharing by this system.**

<u>Mitigation:</u> **There is no internal or external sharing by this system.**

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 will be provided by Interactive Voice Response (IVR) telling the caller (veteran/caretaker) that this call will be recorded for quality purpose, the call will then be routed to an agent within the VA Contact Center. Additional methods of notification occur during onsite individual interviews or in writing via the Privacy Act statement on forms and applications completed by the individual. Additionally, the Department of Veterans Affairs also provides notice by publishing the following VA System of Record Notices (VA SORN) in the Federal Register and online.

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

The copy of the VHA Notice of Privacy Practices is provided in Appendix A-6.1. The notice provided by the Interactive Voice Response (IVR) is a digital recording that the Veterans/caretakers listen too once they call into the VA.

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.

Notice will be provided by Interactive Voice Response (IVR) telling the caller (veteran/caretaker) that this call will be recorded for quality purpose, the call will then be routed to an agent within the VA Contact Center.

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.

For VA to provide service, this requires verification of the veteran before service is rendered. There is no other way to verify who the veteran is without asking PHI/PII.

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.

A caregiver/veteran participation on the call is considered to be consenting to VA use of identifier/information.

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?

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

Privacy Risk: There is a potential risk of Screen/Audio Recording of medical records being captured within the system.

Mitigation: This risk will be mitigated by advising the veteran that his medical records will be Recording (Screen/Audio). Also, all recording will be encrypted meeting the FIPS 140-2 compliance.

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.***

Access to VA owned PII/PHI requires supervisor and/or designee approval before any access can be provided. Access is assigned based on the role/position of the individual employee which has been requested by their assigned supervisor and/or designee. Access control measures ensure that the individuals with access to PII/PHI are only granted access to those options that they have a need to know in the course of their assigned duties.

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

The system is not exempt from the access provisions of the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

The system is a Privacy Act system.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Call/screen recordings s are being recorded for accuracy and cannot be edited or modified.

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.

Recordings cannot be edited or modified.

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.

Calabrio AQM will be recording calls/screen captures for quality accuracy purpose only. Veteran's/caretakers are not able to access recording since this is internal to VA.

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: The risk would be ensuring that only certain members of the organization have access to view the recordings. Example would be supervisors, executive leadership and the team that provides administrative oversight for Calabrio. Calabrio mentioned that supervisors can share the recording and score results with team members. I would suggest that front line team members do not have the ability to share (forward) or screen capture the information on the screen.

Mitigation: This risk is mitigated by Unified Communications Security Division doing a quarterly elevated privilege review of all users with administrative rights. It is also recommended that the contact centers complete a periodically review of who has access to view the recordings to ensure that only those with a need to the information has access.

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.

Calabrio AQM uses a file system Access Control List (ACL) that holds entry that specify individual users or groups to the objects such as files, processes, and programs. Calabrio AQM ACL has an entry for each user that defines the user's privileges. Calabrio AQM will be configured to use single sign on, and this will be accomplished by using Active Directory Federation Service (ADFS).

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?

Users from other agencies do not have access to the system.

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.

System Administrators, Managers, and supervisors will assign agents roles per each agent’s position. Basically, Windows uses Discretionary Access Control List (DACL) which restrict access and System Access Control List (SACL) audits access. As with Windows, Linux provide user, groups, ACL (read, write, executable permission). Microsoft Azure provides the following ACL “Storage Blog Data owner, Storage Blog Contributor, Storage Blog Reader”.

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.

Contractor will have access in designing and maintaining sustainment to the Calabrio AQM solution, per the approved contract. All work completed by the contractors will be within the VA firewall and no VA owned PII/PHI will be shared outside of the VA network. Contractor’s will not have access to PII/PHI. VA SQL database will be maintained by the VA SQL database team (SQL Server Operations, Office of Information Technology).

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.

The system identifies personnel with significant information system security roles and responsibilities. (i.e., system managers, system administrators, contracting staff), documents those roles and responsibilities, and provides appropriate additional information system security training. Security training records will be monitored and maintained. The Talent Management System offers the following applicable privacy courses:

VA 10176: Privacy and Information Security Awareness and Rules of Behavior
VA 10203: Privacy and HIPPA Training
VA 3812493: Annual Government Ethics.
VA 31167: Privacy and Information Security Awareness and Rules of Behavior-Print
VA 3847875: Training Reciprocity-Annual Privacy and Information Training
VHA 3185966: VHA Mandatory Training for Trainees
VHA 3192008: VHA Mandatory Training for Trainees-Refresher
VA 10203: Privacy and HIPPA Training
VA 10204: Privacy and HIPPA Training-Print
VA 20152: Mandatory Training for Transient Clinical Staff

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

8.4a If Yes, provide:

1. *The Security Plan Status:* **Complete**
2. *The System Security Plan Status Date:* **June 12, 2023**
3. *The Authorization Status:* **Authorization to Operate (ATO)**
4. *The Authorization Date:* **May 29, 2023**
5. *The Authorization Termination Date:* **May 1, 2025**
6. *The Risk Review Completion Date:* **March 27, 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. VA Enterprise Cloud Microsoft Azure Government Cloud will be used to archive the media file once the Calabrio AQM reaches the pre-defined threshold for transfer.

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.*

Yes, in accordance with Enterprise Cloud Contract – NNG15SD22B VA118-17-F-2284; Microsoft Enterprise Agreement – GS-35-F-0884P VA118-17-F-1888 re to enter the description.

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.

Yes, the Cloud Service Provider will collect additional data related to the quality and protection of the service they are providing and those will be owned by the VA in accordance with the contracts.

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.

Yes, in accordance with Enterprise Cloud Contract – NNG15SD22B VA118-17-F-2284; Microsoft Enterprise Agreement – GS-35-F-0884P VA118-17-F-1888 re to enter the description.

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).

No. Not Applicable

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Tonya L.
Facemire 234776

Digitally signed by Tonya L.
Facemire 234776
Date: 2023.10.18 10:01:34 -04'00'

Privacy Officer, Tonya Facemire

CHIRAG PATEL

Digitally signed by CHIRAG
PATEL
Date: 2023.10.18 10:17:58
-04'00'

Information Systems Security Officer, Chirag Patel

BRADLEY MILLS

Digitally signed by BRADLEY
MILLS
Date: 2023.10.18 11:23:35 -04'00'

Information Systems Owner, Bradley Mills

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).

Site Type: VBA/VHA/NCA or Program Office	***Applicable NOPPs***
VHA	**Notice of Privacy Practices** **VHA Privacy and Release of Information:**
VBA	VBA Privacy Statement on VA Forms: PRIVACY ACT INFORMATION: The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 38, Code of Federal Regulations 1.576 for routine uses (i.e., civil or criminal law enforcement, congressional communications, epidemiological or research studies, the collection of money owed to the United States, litigation in which the United States is a party or has an interest, the administration of VA Programs and delivery of VA benefits, verification of identity and status, and personnel administration) as identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA, published in the Federal Register. Your obligation to respond is required to obtain or retain benefits. VA uses your SSN to identify your claim file. Providing your SSN will help ensure that your records are properly associated with your claim file. Giving us your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by Federal Statute of law in effect prior to January 1, 1975, and still in effect. The requested information is considered relevant and necessary to determine maximum benefits under the law. The responses you submit are considered confidential (38 U.S.C. 5701). Information submitted is subject to verification through computer matching programs with other agencies.
NCA	**VA Form 40-0247** **VA Form 40-1330** **VA Form 40-1330M**

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