Privacy Impact Assessment for the VA IT System called:

Calabrio Enterprise Contact Center
IT Operations and Services (ITOPS), Office of Information and Technology (OIT)

Date PIA submitted for review:

March 12, 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.Grewal@va.gov	(202)-632-7861
Information System Security Officer (ISSO)	Karen McQuaid	Karen.McQuaid@va.gov	(708) 724-2761
Information System Owner	Brian Mahlum	Brian.Mahlum@va.gov	(360) 759-1909

Abstract

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

The Calabrio Enterprise Contact Center (ECC) will provide Advance Quality Management (AQM), Workforce Management (WFM) and Analytics solution. The AQM solution will improve VA Call Center customer satisfaction and manage call center agent performance.

The AQM solution shall provide the ability to capture voice/screen recording and provide real-time monitoring.

The WFM solution will forecast staffing, and to manage agents scheduling.

The Analytics solution will provide the ability monitor and review performance from the agent's and caller perspective. The Analytics solution utilize speech, text and desktop, along with support additional language such as Spanish.

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*

- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?*
- *Does the system use cloud technology? 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.*
- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*
- *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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

System Name: Calabrio Enterprise Contact Center (ECC)

Program Office: ITOPS OIT

Business Purpose: 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.

Expected Number Individuals: The build out of the system at this time is for 12K VA contact center agents. The information that will be stored will be the interaction of veteran's/spouse and the VA contact center agents.

System Location: The Calabrio ECC will be located the four (4) Trusted Interconnection Connection (TIC) 'Sterling, VA, San Jose, CA, Chicago, IL and Dallas, TX. Primary Core equipment Dallas, TX with Standby Core Chicago, IL.

Description Information IT System: The Calabrio ECC will be integrated with the VA contact center which will provide both inbound and outbound audio/screen recording. These recordings will be the interaction between the veteran/spouse and call center agents which could potentially have identifiable information (PII and PHI).

Information sharing between systems: N/A

PII Maintained: PII/PHI will be maintained at TIC South and North utilizing media file standard storage (SQL server) utilizing encryption that meets FIPS 142-2. VA Microsoft Azure will be used to archive the media file once the Calabrio ECC reaches the pre-defined threshold for transfer. VA Microsoft Azure Federal compliance (https://docs.microsoft.com/en-us/compliance/regulatory/offering-home)

Citation Operate IT System: Equipment has not been installed yet (New System).

PIA Changes Business: N/A

PIA Changes Technology: N/A

Modified/SCORN exists: N/A

Cloud Technology: VA Microsoft Azure will be used to archive the media file and is FedRAMP/FIPS 140 validation. Federal Information Processing Standard (FIPS) 140 Validation - Windows security | Microsoft Docs

Disclosed information: PHI/PII information disclosed will impact the veteran/spouse "HIGH"

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.

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☒ Emergency Contact Information (Name, Phone

Number, etc. of a different individual)
☐ Financial Account Information
☒ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers

☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Current Medications
☐ Previous Medical Records
☐ Race/Ethnicity
☒ Tax Identification Number

☒ Medical Record Number
☐ Other Unique Identifying Number (list below)

PII Mapping of Components

Calabrio ECC consists of 36 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Calabrio ECC and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) 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
VAPNSFONWOEAPA1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWOEAPA2	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWOEAPA3	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWOEABA1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWOEAPB1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWOEAPB2	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWOEAPB3	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWOEABB1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWOEAPO1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWOEAPO2	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWOEAPO3	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit

VAPNSFONWOEABO1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONWOEAPA1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONWOEAPA2	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONWOEAPA3	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONWOEABA1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONWOEAPB1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONWOEAPB2	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONWOEAPB3	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONWOEABB1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONWOEAPO1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONWOEAPO2	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONWOEAPO3	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONWOEABO1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONWOVAPB1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONWOVAPB2	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNNFONWOVABB1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNEFONWOVAPC1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNEFONWOVAPC2	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNEFONWOVABC1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWOVAPA1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWOVAPA2	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNSFONWOVABA1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNWFONWOVAPD1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNWFONWOVAPD2	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit
VAPNWFONWOVABD1	Yes	No	Name, address, phone, DOB, SSN, Medical information	Quality Management and Coaching.	Encryption at Rest and In Transit

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

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

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

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

Information will be collected for the purpose of identifying the veteran/caretaker for medical and benefits.

Information source (veteran/caretaker) will be recorded by the Calabrio-ECC solution for the purpose of supporting the veteran/caretaker requirements.

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 ECC analytics platform will to transform every veteran's interaction into usable data for evaluation.

1.3 How is the information collected?

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

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

Audio/Screen recording is collected by Calabrio-ECC. 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

such evaluating agent performance, ensuring accuracy information that is being provide to the veteran/caretaker.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose. This question is related to privacy control AP-2, Purpose Specification.

The information that is being recorded are used for quality accuracy, ensuring that the veterans/caretakers are getting the best care. VA management will review the recording for evaluation purpose to improve the agent performance and to verify the accuracy of the information that is being given to the veterans.

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

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

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

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 there requirements on how often they will review recordings for quality/evalution purpose.

1.6 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

Per SORN 24VA10A7/85 FR 62406, 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. 2020-21426.pdf (govinfo.gov)

Per SORN 180VA10D/83 FR 64935, 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. 2018-27334.pdf (govinfo.gov)

Per SORN 58VA21/22/28, This system contains records relating to the administration of claims of veterans, servicemembers, reservists, their spouses and dependents for a wide variety of Federal veteran's benefits. 2019-02315.pdf (govinfo.gov)

1.7 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.

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.

Yes, the information is relevant and necessary in identifying veteran/caretaker.

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 ECC resides entirely within VA domain and firewalls, with a URL link to Microsoft Azure for archiving. The Calabrio ECC 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
Branch of Services	Used as a 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?

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The system will not make or create unutilized information. The Calabrio ECC will not have the ability to alter any information that is being recorded. No recording will be placed in an individual's record. 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 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

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

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

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

Add answer here:

Access to PII will be managed by VA and will follow VA standards. Access can be defined to a granular level and should be managed by Business managers within their own Business units. They should not have access to Groups outside of their team unless they are designated as an Administrator and scoped accordingly. Overall, these controls will have to be defined by OIT and Business Unit. Training will be provided to VA Administrator.

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 ECC will be retaining audio/screen recording (SSN, name, DOB, address, medical record, Health Insurance, 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.
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)? If so please indicate the name of the records retention schedule.

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

<<ADD ANSWER HERE>>

3.4 What are the procedures for the elimination of SPI?

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

All recordings are retained until they reach their retention time defined within the retention rules section of the Calabrio ECC solution. Once a recording has reached retention the media is permanently deleted along with the associated call data record.

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

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

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 ECC 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.

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

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

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

<u>Principle of Data Quality and Integrity:</u> Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: Unauthorized access

Mitigation: The recording are encrypted and access is control by two factor authorization.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Information will not be shared	N/A	N/A	N/A
N/A	N/A	N/A	N/A

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Follow the format below:

Privacy Risk: Calabrio ECC audio/screen recording require encryption and access being control.

Mitigation: Calabrio ECC is FIPS-140-2 compliant. Access to the recordings requires two-factor-authentication and privileges are controlled by Access Control List (ACL).

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: This question is #7 in the Privacy Threshold Analysis.

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 data element types such as PII/PHI that are shared/received 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

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

Section 6. Notice

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

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

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

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

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

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.

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> Potential risk of Screen/Audio Recording of medical records

Mitigation: Advising the veteran that his medical records will be Recording (Screen/Audio). Also, all recording will be encrypted meeting the FIPS 140-2 compliant.

Section 7. Access, Redress, and Correction

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

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

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

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

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

N/A-recording cannot be edited or modified.

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

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

N/A- call/screens are being recorded for accuracy.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that

even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

N/A-recording 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.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

Calabrio ECC will be recording calls/screens for quality accuracy purpose only.
Veteran/caretaker 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.

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: 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: factor would be for the contact centers to periodically review 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?

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

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

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

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

Calabrio ECC 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 ECC ACL has an entry for each user that defines the user's privileges. Calabrio ECC will be configured to use single sign on, and this will be accomplished by using Active Directory Federation Service (ADFS). System Admin, 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 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 ECC solution. Contractor's will not have access to PII/PHI. VA SQL database will be maintained by the VA SQL database team (OIT/DevSecOps/IO).

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.

Contractor Training: **Privacy and Information Security and Rules of Behavior Training**; (10176)
Privacy & HIPAA Training; (10203)
Information Security and Privacy Role-Based Training for System Administrator (WBT)

VA employees: **Government Ethics (3812493)**
VA Privacy and Information Security Awareness and Rules of Behavior (10172)
VA Core Values (3901227)

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

If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted,*
2. *Whether it was a full ATO or ATO with Conditions,*
3. *The amount of time the ATO was granted for, and*
4. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

In Process, anticipated date Mid-May 2021

Section 9. 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 Privacy Officers

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

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2021.03.19 08:08:03 -04'00'

Privacy Officer

Signature of Information Security Systems Officers

The Information Security Systems Officers below attest that the information provided in this Privacy Impact Assessment is true and accurate.

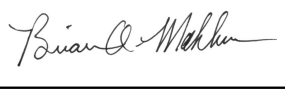
Karen A. McQuaid
321576

Digitally signed by Karen A. McQuaid
321576
Date: 2021.03.19 09:27:29 -05'00'

Information Security Systems Officer

Signature of Area Manager

The Area Manager below attests that the information provided in this Privacy Impact Assessment is true and accurate.



Digitally signed by brian a mahlum
374394
Date: 2021.04.12 12:42:26 -07'00'

System Owner