Privacy Impact Assessment for the VA IT System called:

Genesys Cloud CX -e

Office of Information & Technology

Unified Communications

2539

Date PIA submitted for review:

7/18/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.Drake@va.gov OITPrivacy@va.gov	202-632-8431
Information System Security Officer (ISSO)	Martin DeLeo	Martin.DeLeo@va.gov	202-299-6495
Information System Owner	Scottie Ross	Scottie.Ross@va.gov	478-595-1349

Abstract

The abstract provides the simplest explanation for "what does the system do?".

Genesys Cloud CX is a cloud-based contact center solution providing scalable voice, text, chat, video, and email functionality to connect Veterans in crisis with appropriate Veteran Crisis Line team members. This system assists with advancing the services of the Veteran Crisis Line by providing a full scope of contact center services as well as applying new capabilities to assist with Workforce Optimization/Management and quality management opportunities. The solution provides a means to integrate with VA's Customer Relationship Management (CRM) system. The system includes omnichannel capabilities, Workforce Management (WFM), Workforce Optimization (WFO), Quality Assurance (QA), ability to interface with current and future state systems, and storage and networking infrastructure to support their data centers.

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. What is the IT system name and the name of the program office that owns the IT system?

Genesys Cloud CX is Software as a Service (SaaS) that will be controlled by the Unified Communications program office.

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

The system is a cloud-based contact center solution providing voice, text, chat, video and email functionality that can support 2,000 agents and 500 supervisors, with the ability to grow to 3,500 agents and 1,000 supervisors. There is a need for omnichannel capabilities, Workforce Management (WFM), Workforce Optimization (WFO), Quality Assurance (QA), ability to interface with current and future state systems, and storage and networking infrastructure to support their data centers. The solution will provide a means to integrate into VA's Customer Relationship Management (CRM) system.

C. Who is the owner or control of the IT system or project?

The system is owned and operated by the providing SaaS vendor Genesys and will be controlled by the Unified Communications program office.

2. Information Collection and Sharing

D. What is 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 over 2,000 VA Veteran Crisis Line employees. The information that will be stored will be the interaction of veteran's/spouse and the Veteran Crisis Line employees. The Veteran Crisis Line (VCL) currently receives roughly over a million

calls per year so the system has the capability of recording roughly the same of amount of Veteran data, which will be retained for 4 years.

E. What is 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, medications, addresses, personal email, Date of Birth, Military History/Service, and medical record number. 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. What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.

The Genesys CX Cloud -e shares information within the VA for Healthcare treatment coordination and emergency response. These internal organizations can be found in Section 4 of the PIA.

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

The Genesys Cloud CX Continuity Management and Service Reliability Engineering teams have configured AWS to perform backups for the Genesys Cloud CX information system. The Service Reliability Engineering team configures Genesys Cloud CX databases to replicate across three nodes. One node serves as the primary node, while the other nodes serve as secondary and standby nodes.

Data stored in S3 is replicated using locally redundant storage protections built into AWS and replicated across availability zones as configured by the Service Reliability Engineering team.

Amazon Machine Images (AMIs) are automatically backed up using Amazon Elastic Block Storage (EBS) snapshots. The Service Reliability Engineering team configures AWS to store daily EBS snapshots in an S3 bucket and retain a minimum of three previous versions. DevOps stores infrastructure code in version controlled Bitbucket repositories, which are automatically replicated into an S3 bucket.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

146VA005Q3/73 FR 16093 Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008) https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf

- 146VA005Q3/73 FR 16093 Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008) https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf
- 24VA10A7, Patient Medical Records-VA (10/2/2020) https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf
- 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (12/23/2020) https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

- 90VA194, Call Detail Records-VA (3/15/2024) https://www.govinfo.gov/content/pkg/FR-2024-03-15/pdf/2024-05535.pdf
- 113VA10, Telephone Service for Clinical Care Records-VA (5/10/2023) https://www.govinfo.gov/content/pkg/FR-2023-05-19/pdf/2023-10732.pdf 11.pdf
- 158VA10 Veterans Crisis Line Database – VA 6/12/2023 https://www.govinfo.gov/content/pkg/FR-2023-06-12/pdf/2023-12401.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?

No. This system is not in the process of being modified.

4. System Changes

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

No. No changes in the business processes will occur.

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

No. No changes in our technology will occur.

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. It must also match the information provided in question 3.4 of the PTA.

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[1]
☐ 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)

Other PII/PHI data elements: VA Employee Email Address and VA User ID

PII Mapping of Components (Servers/Database)

Genesys Cloud CX -e consists of **1** key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Genesys Cloud CX -e** 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 server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	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
Azure Synapse/Dedicated SQL Pool	**Yes**	Yes	SSN Date of Birth Name	Call Detail reporting data for quality control and	Raw data is secured in a secure file location that ensures data is secured with FIPS-validated cryptography

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

				data analytics	

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

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

Information will be collected for the purpose of identifying the veteran/caregiver for medical assistance. Information is being collected from other systems.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.
The other sources of information that will be captured within the screen captures will include VA sensitive data from VISTA/CPRS, and MedoraForce. All other data will be provided from the Veteran/Caregiver over the duration of the phone call that will be captured in the call recordings.

1.2c Does the system create 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. Quality management reviews will be completed and documented within the system.

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

Audio/Screen recording is collected by Genesys CX Cloud -e. 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. The system will arrange the recordings and screen captures by date/time/group.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is 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 personnel 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 Does the system check 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

- Veterans' Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.
- Freedom of Information Act (FOIA) 5 USC 552
- VHA Directive 1605.01 Privacy & Release of Information
- VA Directive 6500 Managing Information Security Risk: VA Information Security Program.

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Genesys CX Cloud -e collects Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI), such as Protected Health Information (PHI). 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. Any unauthorized access may result in the unsanctioned change in information that may lead to creation of inaccurate data that is not relevant or necessary to assist with providing care. Unauthorized access may result in the disruption of services which could lead to incomplete data being assessed in order to provide continuity of care. Unauthorized access could result the disruption of services that prevents the system from attaining any new/current information.

Mitigation: Genesys CX Cloud -e employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include access control, awareness and training, audit and accountability, certification, accreditation, and security assessments, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, systems and services acquisition, system and communications protection, and system and information integrity. The boundary employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives. The system employs access control mechanisms that only allow approved end users and elevated privilege users access to system on a "Need to Know" basis. This access is reviewed in accordance with VA Handbook 6500 control requirements. The system also employ's different

roles within the system which align to the separation of duties requirements. Only those with a need to access the data directly, and potentially delete or alter data, will be approved within a VA approved access control request process such as Electronic Permission Access System (EPAS). All VA owned sensitive data is encrypted in transit, at rest and in use using FIPS 140-2 (or successor) encryption.

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 that 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.

PII/PHI Data Element	Internal Use	External Use
Name	Used to identify the Veteran in crisis	No External Use
Social Security Number	Used as a patient identifier	No External Use
Date of birth	Used to identify age and confirm patient identity.	No External Use
Personal Mailing Address	Used for communication, and potential coordination of emergency services	No External Use
Personal Phone Number	Used for communication, and potential coordination of emergency services	No External Use
Personal E-mail Address	Used for communication, and potential coordination of emergency services	No External Use
Medications	Used within the medical records for health care purposes/treatment.	No External Use
Medical Records	Used for continuity of health care.	No External Use
Gender	Used to confirm patient identity	No External Use
Military History/Service Connection	Used to identify the Veteran in crisis and provide potential crisis support.	No External Use
VA email Address	Part of the call recording	No External Use
VA User ID	Part of the call recording	No External Use
Name of VA Employee (listed as name on table in 1.1)	Part of the call recording	No External Use

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.
The system will employee monitoring and security auditing tools that will monitor the system for compliance with VA Handbook 6500 security controls, such as Splunk and Nessus. The data that will be produced from these monitoring and security auditing tools will involve access control measures and disruption of services type of data that will be used to ensure the system maintains continuous and uninterrupted services. Azure Synapse will be used to analyze the raw data of the phone calls received to ensure accuracy of the data and provide metrics to the VHA Organization using the system.

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 Genesys CX Cloud -e 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 Genesys CX Cloud -e, a new recording will be created, archived, and organized by the data/time/group it was received. Only action that will be taken will be identifying the reason for the veteran/caregiver call. VA managers will have access to the recording. VA managers will have the ability to allow the VA agent who took the call the ability to listen to the recording for evaluation purpose. Call recordings and screen captures will be accessible by searching by the date and time of the call that was received. They will not be added to any other record as they are solely used for Workforce Management purposes. The retention of the audio recordings aligns with 158VA10, Veteran Crisis Line Records-VA and VHA Records Control Schedule 10-1, Item Number 1930.1.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.
2.3a What measures are in place to protect data in transit and at rest?

The Genesys Cloud CX Continuity Management and Service Reliability Engineering teams have configured AWS to perform backups and store user-level and system-level data using Amazons S3 default encryption to protect the confidentiality and integrity of all backed up information. AWS leverages TLS 1.2 or better encryption for protecting information in-transit,

and 256-bit Advanced Encryption Standard (AES) symmetric encryption for all data-at-rest. Genesys Cloud CX and relevant backups are distributed across multiple Availability Zones to protect the availability of backup data.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
Access to PII is limited by the Cloud service to only those data items deemed necessary to perform their job, as determined by their management team and job description. Access to the Cloud service is by PIV authentication. Individual administrator user IDs and access are provided only based on need. The Veteran Crisis Line (VCL) limits access rights and controls only to valid end users. Rigorous security monitoring controls are in place to prevent unauthorized access and intrusion, and to protect all information. Furthermore, on an annual basis, all end users are required to take VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176), Privacy and HIPAA Training (VA 10203). The VA IT office is responsible in assuring safeguards for the PII. VHA ensures that the practices stated in the PIA are reinforced by requiring Contractors and VA employees to complete all VA trainings: VA Privacy and Information Security Awareness and HIPAA.

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 show 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 Account Provisioning Deprovisioning System. Access Control measures will be addressed in the corresponding Access Control (AC) Standard Operating Procedure (SOP) that include creation and removal of access and the approval authority for each account type.

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; as well as regular audits of individuals accessing sensitive information. Access to the system is monitored and audited by the vendor (Genesys CX Cloud) and by the Office of Information Security (OIS). The Genesys security team will audit the system for unusual activity and unexpected device types on a weekly basis. The OIS Enterprise Security Operations (ESO) ISSOs will audit end user access on a monthly basis to ensure only active accounts have access to the VA system and to the Genesys CX Cloud system. Access logs to the VA network are also reviewed by the Infrastructure Operations (IO) Domain Infrastructure (DI) team through automated alert mechanisms that monitor Active Directory accounts on a daily basis.

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

The data owners, system owner and system key stakeholders are responsible for ensuring the safeguards for the PII.

Section 3. Retention of Information

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

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system.*

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

- Name
- Social Security Number (SSN)
- Date of Birth
- Phone Numbers
- Medical records
- Mailing Address
- Email Address
- Military History/Service Connection
- Medications
- Gender
- VA Email Address
- VA UserID

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.*

General Record Schedule, section 6.5 Public Customer Service Records, **Temporary.** Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate. Disposition Authority: DAA-GRS-2017-0002-0001 https://www.archives.gov/records-mgmt/grs.html

DAA-GRS-2017-0002-0001: https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs-2017-0002_sf115.pdf

Veteran Health Administration Record Control Schedule (RCS)10-1, 1925- Public Customer Service Records Including Call Centers, 1925.1, Temporary. Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate. Disposition Authority GRS 6.5, item 020 DAA-GRS 2017-0002 0001 https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf

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 are stored within the system of record indicated on an approved disposition authority.

General Record Schedule, section 6.5 Public Customer Service Records, **Temporary.** Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate. Disposition Authority: DAA-GRS-2017-0002-0001 https://www.archives.gov/records-mgmt/grs.html

DAA-GRS-2017-0002-0001: https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs-2017-0002_sf115.pdf

Veteran Health Administration Record Control Schedule (RCS)10-1, 1925- Public Customer Service Records Including Call Centers, 1925.1, Temporary. Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate. Disposition Authority GRS 6.5, item 020 DAA-GRS 2017-0002 0001 https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf

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

General Record Schedule, section 6.5 Public Customer Service Records, **Temporary.** Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate. Disposition Authority: DAA-GRS-2017-0002-0001 https://www.archives.gov/records-mgmt/grs.html

DAA-GRS-2017-0002-0001: https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs-2017-0002_sf115.pdf

Veteran Health Administration Record Control Schedule (RCS)10-1, 1925- Public Customer Service Records Including Call Centers, 1925.1, Temporary. Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate. Disposition Authority GRS 6.5, item 020 DAA-GRS 2017-0002 0001 https://vaww.va.gov/vhapublications/rcs10/rcs10-1.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 the Department of Veterans' Affairs Directive 6500 VA Cybersecurity Program (2/24/2021). 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 per VA Directive 6500. Digital media is shredded or sent out for destruction per VA Directive 6500.

The Genesys corporate policy "ECS 15 - Mobile Device Security Management Policy" prohibits the use of removable devices. In the rare case a removable device is used, the Genesys IT team marks the removable drive, logs and tracks the Genesys personnel who has checked out the removable device, and encrypts the removable device using Digital Guardian as approved by the AO. Once the removable drive is returned, the Genesys IT team sanitizes the removable device.

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.

No PII/PHI is used to test systems prior to deployment. All testing is conducted with test samples of the required application categorization of the subject. Any potential that may involve PII/PHI are supposed to be reviewed by the systems assigned Privacy Officer (PO) first before any actual presentation can be provided. That training environment (tentative Pre-Production environment) is only available to those with a need to know in the course of their duties. Any information that is provided to a requesting research team must be approved by an ISSO and PO assigned to review such research protocols. That research protocol must also be approved by the governing research board as well as utilize a security transmission and storage method that has been approved for use by the Office of Information Security in accordance with VA Handbook 6500.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the information maintained by Genesys CX -e system 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.

Mitigation: To mitigate the risk posed by information retention, they system 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 Enterprise Contact Center-Avaya 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***
Veterans' Health Administration VistA	Screen captures of the VA employee's desktop screen will be taken and stored within Genesys CX -e for the purpose of monitoring by VCL Leadership and their Quality Management Teams.	Name, Social Security Number Date of Birth Personal Mailing Address Personal Phone Number Medical Records, Medications Email address	Electronically pulled from VistA thru Computerized Patient Record System (CPRS)
MedoraForce	Screen captures of the VA employee's desktop screen will be taken and stored within Genesys CX -e for the purpose of monitoring by VCL Leadership and their Quality Management Teams.	Name, Social Security Number Date of Birth Personal Mailing Address Personal Phone Number Medical Records, Medications Email address	Manually input by the VCL Crisis Responder during the call
Customer Experience Insights (CXI)	Raw data from Genesys CX -e will be transferred and stored for Call Detail/Quality records, as well as used by the VCL for data analytics.	Social Security number (last 4) Name Date of Birth	Electronic transferred from Genesys to CXI via HTTPS/Port 443.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The internal sharing of data is necessary for the individuals to receive proper healthcare and benefits within the VA. However, there is a risk that the data could be shared with an inappropriate VA organization or institution which could result in a breach of privacy and disclosure of PII/PHI to unintended parties or recipients.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted. Also, the removal of any call recording and/or screen captured requires an individual to be assigned a specific role, which is only authorized by the supervisory authority of that specific organization. No unauthorized role will be able to remove any data from the system.

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***
Genesys Cloud	Call recordings and screen captures, that contain the PII/PHI, will be stored on Genesys CX - e.	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number, Medical Records, Medications, Email address, Gender, Military History/Service Connection	MOU-ISA (Tentative)	VPN S2S

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.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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: The sharing of data is necessary for individuals to receive health care assistance from the Department of Veteran's Affairs. However, there is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation: Safeguards implemented to ensure data is not shared inappropriately with organizations are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know purposes, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption and access authorization are all measures that are utilized within the administrations. Standing letters for information exchange, business associate agreements and memorandums of understanding between agencies and VA are monitored closely by the Privacy Officer (PO), ISSO to ensure protection of information.

All personnel accessing Veteran's information must first have a successfully adjudicated background screening or Special Agreement Check (SAC). This background check is conducted by the Office of Personnel Management A background investigation is required commensurate with the individual's duties.

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.

Yes, a notice is provided to the individual before collection of the information, either by mail to their home address or received in person while visiting a VHA Facility. The

VHA Notice of Privacy Practices is also electronically available here: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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

A notice is provided.

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.

This Privacy Impact Assessment (PIA) also serves as notice of the Genesys CX -e system. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." The Veteran's/Caregivers are also notified on the call, in accordance with VHA Directive 1078, that the call is being monitoring and recorded for quality control. The VHA Notice of Privacy Practices, which is provide to the Veteran in different methods described above, states on page 4:

Serious and Imminent Threat to Health and Safety. We may use or disclose your health information without your authorization when necessary to prevent or lessen a serious and imminent threat to the health and safety of the public, yourself, or another person. Any disclosure would only be to someone able to help prevent or lessen the harm, such as a law enforcement agency or the person threatened. You will be notified in writing if any such disclosure has been made by a VHA health care facility.

The VHA Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected health information to individuals interacting with VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans.

Employees and contractors are required to review, sign, and abide by the National Rules of Behavior on an annual basis.

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.

No. 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. In accordance with VHA Directive 1078, Privacy of Persons Regarding Photographs, Digital Images and Video or Audio Recordings: *"Ensuring that any operating Call Center notify persons if calls will be subject to monitoring or recording and how any recording will be used. Such notice is sufficient to establish consent by participants on the call to the monitoring, recording and use of any recording. NOTE: Call Center operators do not need to obtain a*

signed VA Form 10-3203, Consent for Production and Use of Verbal or Written Statements, Photographs, Digital Images and/or Video or Audio Recordings by VA, from participants."

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.

Yes. A caregiver/veteran participation on the call is consenting to VA use of identifier/information. This is due to consent for call centers is established once the caller has listened to the automated message stating the call will be monitored and recorded for quality purposes. If the caller no longer consents, they can hang up.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: There is a risk that veterans and other members of the public will not know that the Genesys CX -e system exists or that it collects, maintains, and/or disseminates PII, PHI or PII/PHI about them.

Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans are enrolled for health care. s. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SOR) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

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.

X The call recordings and screen captures are maintained by date and time stamp and are accessible via a FOIA request. The individual would have to provide a written request to the appropriate FOIA Officer to request a copy of the call recordings and/or screen captures.

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

The call recordings and screen captures are maintained by date and time stamp and are accessible via a FOIA request. The individual would have to provide a written request to the appropriate FOIA Officer to request a copy of the call recordings and/or screen captures. The website: Freedom of Information Act (va.gov) provides "How to instructions" on how to request a FOIA request. FOIA request can be filed electronically here: VA Public Access Link-Home (efoia-host.com) or by mail or fax requests to:

Department of Veterans Affairs
Freedom of Information Act Services (005R1C)
811 Vermont Avenue, NW
Washington, DC 20420
Office: 1-877-750-3642
Fax: 202-632-7581

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 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 not exempt from access provisions of the Privacy Act.

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.

There are not procedures for correcting inaccurate or erroneous information. Call/screen recordings 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.

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) which states:

Right to Request Amendment of Health Information.

You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.

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

- File an appeal
- File a "Statement of Disagreement"
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***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.
In order to gain access to the call recordings and screen captures, a Freedom of Information Act (FOIA) request would need to be submitted by the individual to gain access to the call recordings and/or screen captures. The request would need to be pulled by the date and time of that the call took place.
.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: The system mitigates the risk of incorrect information in an individual's records by authenticating information when possible, using the resources discussed in question 1.5. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.

As discussed in question 7.3, the NOPP, which every enrolled Veteran receives every three years or when there is a major change. The NOPP discusses the process for requesting an amendment to one's records.

Individuals assigned to the VHA Release of Information (ROI) office are available to assist Veterans with obtaining access to their health records and other records containing personal information. The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

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

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

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

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

Individuals receive access to the system by gainful employment in the VA or upon being awarded a contract that requires access to the boundary systems. Upon employment, the Office of Information & Technology (OI&T) creates computer and network access accounts as determined by employment positions assigned. Users are not assigned to software packages or network connections that are not part of their assigned duties or within their assigned work area. The system requires access to the VA network be requested using the local access request system. VA staff must request access for anyone requiring new or modified access to the VA network and/or designated system boundary. Staff are not allowed to request additional or new access for themselves.

Initial Access is requested utilizing Electronic Permission Access Boundary (ePAS) and YourIT User Provisioning. Users submit access requests based on need to know and job duties. Supervisor and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes. Once access is granted, individuals can log into the system(s) through dual authentication, i.e., a PIV card with a complex password combination. Once inside the system, individuals are authorized to access information on a need-to-know basis.

Once the individuals are granted access to the overall VA network, the VHA organization that utilizes the system will assign access based on the role and/or job description of that individual end users, i.e., Supervisors will have supervisory access and data analytics folks with have access to controlling analytic workflows.

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?

All end users with access to the system are VA employees and/or VA contractors.

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.

Veteran Crisis Line (VCL) employees will have roles assigned based on their assigned duties and will be granted access based on the “Least Privilege” model so that they only have access data that they “Need to Know in the course of their duties.

OIT Employees and contractors will have administrator roles assigned to design, operate and troubleshoot the system throughout the duration of the systems lifecycle. Their access will be approved via the MyVA EPAS process in order to gain appropriate administrator rights to the system.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Contractors will have access to the system after completing the VA Privacy and Information Security Awareness training and Rules of Behavior annually, and after the initiation of a background investigation. Contractors are only allowed access for the duration of the contract this is reviewed by the privacy officer and the designated Contracting Officer Representative (COR). Per the Contractors On/Off Boarding (CONB) process, contractors can have access to the system only after completing mandatory information security and privacy training, Privacy and HIPAA Focused Training as well as having completed a Special Agency Check, finger printing and having the appropriate background investigation scheduled with Office of Personnel Management. Certification that this training has been completed by all contractors must be provided to the employee who is responsible for the contract in question. In addition, any of the contractors with elevated privileges will also be asked to complete additional training and submit a request for the specific administrative access that is required as part of the contract. Contractors with VA network access must have an approved computer access request on file. The system owner, or designee, in conjunction with the ISSO and the applicable COR reviews accounts for compliance with account management requirements. User accounts are reviewed periodically in accordance with National schedules. A Business Associate Agreement (BAA) will be completed that discusses the vendors role in adhering to HIPAA requirements as well as define their role in ensuring that the privacy of the VA owned sensitive information is maintained.

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, end users, 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 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:* Completed
2. *The System Security Plan Status Date:* May 31st, 2023
3. *The Authorization Status:* FedRAMP Authorized
4. *The Authorization Date:* 6/26/2023
5. *The Authorization Termination Date:* VA ATO not yet granted.
6. *The Risk Review Completion Date:* Still pending.
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.***

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)*

This system is a Software as a Service (SaaS) that uses cloud technology. The system is currently FedRAMP Authorized and active on the FedRAMP Marketplace under FedRAMP ID FR2131766015.

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, the contract establishes who has ownership rights over the data including PII. Contract Number is 36C10B22C0030. The contract includes VA Handbook 6500.6 Contract Security Language from Appendix B and C, as well as SaaS specific language provided by the DTC.

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.

No ancillary data will be collected by the Cloud Provider. All data, per VA Contract Security Clause from VA Handbook 6500.6 Contract Security.

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.

The roles and responsibilities of each organization are described within the contract, to include the Security and/or Privacy clause that has been inserted from VA Handbook 6500.6, Contract Security. SaaS Contract Language has also been provided by the Digital Transformation Center (DTC), which clearly defines the roles and responsibilities of the Cloud provider and Department of Veteran's Affair's.

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).

The system does not use RPA.

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**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

JULIE DRAKE Digitally signed by JULIE DRAKE
Date: 2024.07.29 10:48:30 -06'00'

Privacy Officer, Julie Drake

JOHN DELEO Digitally signed by JOHN DELEO
Date: 2024.08.05 09:13:00 -04'00'

Information System Security Officer, Martin DeLeo

SCOTTIE ROSS Digitally signed by SCOTTIE ROSS
Date: 2024.08.05 09:35:47 -04'00'

Information System Owner, Scottie Ross

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; screen shot of a website collection privacy notice).

Notice Documents:

- 146VA005Q3/73 FR 16093 Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008)
- https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf
  24VA10A7, Patient Medical Records-VA (10/2/2020)
  https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf
- 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (12/23/2020) https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf
- 90VA194, Call Detail Records-VA (3/15/2024)
  https://www.govinfo.gov/content/pkg/FR-2024-03-15/pdf/2024-05535.pdf
- 113VA10, Telephone Service for Clinical Care Records-VA (5/10/2023)
  https://www.govinfo.gov/content/pkg/FR-2023-05-19/pdf/2023-10732.pdf
  158VA10 Veterans Crisis Line Database – VA 6/12/2023
  https://www.govinfo.gov/content/pkg/FR-2023-06-12/pdf/2023-12401.pdf

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

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