Privacy Impact Assessment for the VA IT System called:

Google Services

Veterans Affairs Central Office

Unified Communications

eMASS ID #TBD

Date PIA submitted for review:

December 20, 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	Harris Khan	Harris.Khan2@va.gov	703-789-7883

Abstract

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

Google Services offers two components, Dialogflow and CCAI (Contact Center Artificial Intelligence). These two Software as a Service (SaaS) solutions act as a natural language understanding (NLU) virtual agent platform that takes human language from text or voice conversations and translates it into actions such as providing information, locating/transferring to additional support, allowing a user to complete a task, etc. For a user, speaking with a virtual agent is similar to speaking with a human call center agent. The platform will be integrated with CISCO - VA's existing Interactive Voice Response (IVR) platform. That integration will (at minimum) allow Google DialogFlow to collect the conversational input from voice, interpret it and decide on an action (ex: send to a human), submit the interpretation over to CISCO, and CISCO finalizes the triage to the right human agent.

Data is used for authenticating the Veteran caller and loading Veteran's claim's information. Once Veteran caller has been authenticated via providing the requested identifying information, the application can communicate that Veteran's disability compensation claim's status.

Overview

The overview is the most important section of the Privacy Impact Assessment (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 business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

Google Services provides customers 24/7 access to immediate conversational self-service with seamless handoffs to human agents for more complex issues by building virtual agents and interactive voice response (IVR) that can perform tasks, such as scheduling appointments, answering common questions, or assisting a customer with simple requests. This allows the customer to be serviced in a timelier manner while freeing up time for VA employees. This product increases the overall efficiency of the department.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

The system is owned and operated by the providing Software as a Service (SaaS) vendor Google Services and it will be controlled by the Office of Information & Technology (OI&T) Connectivity and Collaboration Services (CCS), Unified Communications program office.

2. Information Collection and Sharing

C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?

To estimate the average number of callers during the first year's proof of concept, we projected an expected volume based on National Contact Center (NCC))/VBA data. This analysis indicated approximately 7 million callers annually. These callers primarily consist of Veterans and third-party individuals supporting Veterans such as fiduciaries and family members. We expect the number to be larger as the modernization expands.

Check if Applicable	Demographic of Individuals
☒	Veterans or Dependents
☒	VA Employees
☐	Clinical Trainees
☒	VA Contractors
☐	Members of the Public/Individuals
☐	Volunteers

D. What is a general description of the information in the IT system and the purpose for collecting this information?

The system will collect Names, Phone Numbers, Social Security Numbers, medications, addresses, personal email, Date of Birth, Military History/Service, and medical record number, benefit claim information, race/ethnicity, vehicle license plate numbers, tax identification information, gender, next of kin, fax numbers, mother’s maiden name and emergency contact information. The purpose for collecting these information types is to assist with identifying the Veteran, faster notification and/or transfer to a human agent to assist with Veteran benefits, as well as to provide accurate and timely assistance in coordinating healthcare treatments and benefits in support to the Veterans.

E. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.

Currently, Google Services receives information from within the VA for Healthcare treatment and Veteran benefits coordination. The information that will be shared with Customer Experience Insights (CXI) are categorized as Call Detail records. This information will be used by the Unified Communications program office to review call quality metrics to ensure continuous uninterrupted communications. It will also be used by the overall project team to analyze gaps in our contact center support and provide feedback.

F. Are the modules/subsystems only applicable if information is shared?

Yes, these subsystems provide the necessary information to assist with authenticating the Veteran and/or caregiver to ensure they receive accurate information or are routed to the correct service representative to assist with their claim. Customer Experience Insights (CXI) is the only subsystem that Google Services will directly share information with during the duration of the call between the Veterans/Caregiver and the VA Employees and VA Contractors.

G. Is the system operated in more than one site to include primary and secondary 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?

Yes, the Google Common Infrastructure uses Google's proprietary distributed file system to store data. The distributed file system provides fault tolerance while running on inexpensive commodity hardware and delivers high aggregate performance to a large number of clients. Data is organized in large structured distributed databases built on top of the distributed file system. Data is stored in the distributed file system and replicated over multiple machines to provide data redundancy. The Google Global Capacity Delivery (GCD) team has created a highly redundant, geographically dispersed network of secure data centers around the world. GCD selects data centers based on a site selection process that includes geographical separation between data centers as a major factor. This reduces the data centers' susceptibility to the same environmental or infrastructure threats or hazards such as weather events, earthquakes or large-scale power outages.

Google hardware, software, and data centers are the same around the world to provide consistent, trusted security, ease maintenance, and offer a transparent solution to customers. The paths of internet traffic frequently change as traffic is routed to meet shifting demand, backbone outages, etc., but Google uses various mechanisms to ensure traffic is encrypted in transit.

3. Legal Authority and System of Record Notices (SORN)

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

- 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
- 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.
- Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b)

H. What is the SORN?

23VA10NB3/80FR45590, *Non-VA Fee Basis Records-VA* (7/30/2015)
https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

24VA10A7/85FR62406, *Patient Medical Records-VA* (10/2/2020)
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

34VA10/86FR33015, *Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA* (6/23/2021)
https://www.govinfo.gov/content/pkg/FR-2021-06-23/pdf/2021-13141.pdf

58VA21/22/28/86FR61858, *Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA* (11/8/2021) https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

77VA10E2E/85FR7395, *Health Care Provider Credentialing and Privileging Records-VA* (2/7/2020)
https://www.govinfo.gov/content/pkg/FR-2020-02-07/pdf/2020-02477.pdf

79VA10/85FR84114, *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

89VA10/88FR17639, *Income Verification Records-VA* (3/23/2023)
https://www.govinfo.gov/content/pkg/FR-2023-03-23/pdf/2023-05925.pdf

90VA194/89FR19021, *Call Detail Records-VA* (3/15/2024)
https://www.govinfo.gov/content/pkg/FR-2024-03-15/pdf/2024-05535.pdf

99VA13/74FR14613, *Automated Safety Incident Surveillance and Tracking System-VA* (3/31/2009)
https://www.govinfo.gov/content/pkg/FR-2009-03-31/pdf/E9-7160.pdf

113VA10/88FR32289, *Telephone Service for Clinical Care Records-VA* (5/19/2023)
https://www.govinfo.gov/content/pkg/FR-2023-05-19/pdf/2023-10732.pdf

114VA10/86FR6996, *The Revenue Program Billings and Collection Records-VA* (1/25/2021)
https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf

121VA10/88FR22112, *National Patient Databases-VA* (4/12/2023)
https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

147VA10/86FR46090, *Enrollment and Eligibility Records-VA* (8/17/2021)
https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

168VA005/86FR6975, *Health Information Exchange -VA* (1/25/2021)
https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf

172VA10/86FR72688, *VHA Corporate Data Warehouse-VA* (12/22/2021)
https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf

I. *SORN revisions/modification*
No, no SORN is being updated because of the new services that Google Services will provide.

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.*
The system is not in the process of being modified and the SORN will not require a revision or amendment at this time.

4. System Changes

J. *Will the business processes change due to the information collection and sharing?*

☐ Yes
☒ No

K. *Will the technology changes impact information collection and sharing?*

☐ Yes
☒ No

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 Information 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
☒ **Full** Social Security Number
☒ **Partial** 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/Sex
☐ Integrated Control Number (ICN)
☒ Military History/Service Connection
☒ Next of Kin
☐ Date of Death
☐ Business Email Address
☐ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (list below)

Other PII/PHI data elements: Internal Entry Number (IEN), Claim ID, Patient Internal Control Number (ICN), User ID (Unique to Individual), Account Username

1.2 List 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?

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

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

No information from sources other than the individuals will be required as the system only receives and maintains information from the VA Employee, VA Contractor, Veteran and/or their caregivers.

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

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

The system does not create information. It only processes the information provided by the VA Employee, VA Contractor, Veteran and/or caregiver. The system is not creating a record that includes the information provided by the interaction with the Veteran and/or Caregiver.

1.3 Methods of information collection

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?

The information is collected directly from the Veterans and/or caregiver via interaction with a human agent and/or the Interactive Voice Response (IVR) platform currently in use by the VA. The VA Employee and VA Contractor supporting the VA services will also have information collected as they work on the system and support the Veterans/Caregivers in day-to-day operations.

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?

A form is not used in conjunction with this this system to collect information.

1.4 Information checks for accuracy, and how often will it be checked.

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

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

The Veterans and/or caregivers providing the required information will confirm its accuracy in order to complete the initial stages of the workflow intake process. Any human agent that assists the Veterans and/or caregiver will also confirm the information is accurate prior to completing the process of assisting the individuals. The VA Employees and VA Contractors providing information have confirmed their identity by authenticating into the system via approved credentials as well as providing their own PII to identity themselves to the Veterans/Caregivers.

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?

No, this system does not access a commercial aggregator of information to check for accuracy. The system checks for accuracy by comparing the information provided by the Veteran/Caregiver against what the VA systems currently have listed. Any discrepancies with the information provided or maintained by the VA will be corrected in coordination with working with the Veterans and Caregivers. The VA Employees and VA Contractors providing information will also be confirmed for accuracy by the system during the authentication workflows. Any inaccurate data input into the system will prevent them from accessing the system.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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
- 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.
- Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b)

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:

<u>Principle of Purpose Specification:</u> The collection ties with the purpose of the underlying mission of the organization and its enabling authority.

<u>Principle of Minimization:</u> The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: *The program, to the extent possible and practical, collects information directly from the individual.*

Principle of Data Quality and Integrity: *VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.*
This 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: Google Services 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. If the system did experience a breach by someone with unauthorized access, that individual could delete and/or change information that is needed in order to provide services to the Veterans and/or their caregivers. This would create a delay in necessary Veteran health care services being provided or delay potential benefits from being awarded to Veterans and their caregivers.

Mitigation: Google Services 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, 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 Moderate 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.

All employees with access to Veteran’s health information are required to complete the Privacy and HIPAA Focused training as well as the VA Privacy and Information Security Awareness & Rules of Behavior training annually. The VA enforces two-factor authentication by enforcing smartcard logon requirements. Personal Identity Verification (PIV) cards are issued to employees, contractors, and partners in accordance with Homeland Security Presidential Directive-12 (HSPD-12). The Personal Identity Verification (PIV) Program is an effort directed and managed by the Homeland Security Presidential Directive 12 (HSPD-12) Program Management Office (PMO).

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	Call Recordings and Screen captures on Genesys CX
Full Social Security Number	Used as a patient identifier	Call Recordings and Screen captures on Genesys CX
Partial Social Security Number	Used as a patient identifier	Call Recordings and Screen captures on Genesys CX
Date of birth	Used to identify age and confirm patient identity.	Call Recordings and Screen captures on Genesys CX
Mother's Maiden Name	Used to confirm patient identity	No External Use
Personal Mailing Address	Used to identify the Veteran	Call Recordings and Screen captures on Genesys CX
Personal Phone Number	Used to identify the Veteran	Call Recordings and Screen captures on Genesys CX
Personal Fax Number	Used to identify the Veteran	No External Use
Personal Email Address	Used to identify the Veteran	No External Use
Emergency Contact Information	Used in cases of emergent situations such as medical emergencies.	No External Use
Financial Information	Used to calculate co-payments and VA health care benefit eligibility	No External Use
Health Insurance Beneficiary Numbers Account Numbers	Used to communicate and bill third part Health care plans and to calculate co-payments and VA health care benefit eligibility	No External Use
Certificate/License Numbers	Used to track and verify legal authority to practice medicine and Licensure for health care workers in an area of expertise.	No External Use
Vehicle License Plate Number	Used to confirm patient identity	No External Use
Internet Protocol (IP) Address Numbers	Used to confirm patient identity	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.	Call Recordings and Screen captures on Genesys CX
Race/Ethnicity	Used to confirm patient identity	No External Use
Tax Identification Number	Used for employment, eligibility verification	No External Use
Medical Record Number	Used to confirm patient identity	No External Use
Gender/Sex	Used to confirm patient identity	No External Use
Military History/Service Connection	Used to identify the Veteran in crisis and provide potential crisis support.	Call Recordings and Screen captures on Genesys CX
Next of Kin	Used in cases of emergent situations such as medical emergencies. Used when patient expires and in cases of patient incapacity.	No External Use
Internal Entry Number (IEN)	Used to identify the Veteran and provide associated benefits	No External Use
Claim ID	Used to identify the Veteran and provide associated benefits	No External Use
Patient Internal Control Number (ICN)	Used to identify the Veteran and provide associated benefits	No External Use
User ID (Unique to Individual)	Used to identify the Veteran	Used to authenticate the Veteran/Caregiver on ID.ME and/or Login.GOV
Account Username	Used to identify the VA Employee and VA Contractor	Call Recordings and Screen captures

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

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

The two main cloud Google Services that will be initially used (Dialogflow and Contact Center AI) will allow the VA with the ability to provide Customers 24/7 access to immediate conversational self-service with seamless handoffs to human agents for more complex issues by building virtual agents and interactive voice response (IVR) that can perform tasks, such as scheduling appointments, answering common questions, or assisting a customer with simple requests. Google Services allows for Omnichannel implementation of IVR across multiple platforms. Google Services allows our contact centers the ability to monitor the analytics of their sessions and assist with workforce optimization/management processes that allow them to continuously increase the satisfaction of their customer's experience. It will allow the contact centers the ability to develop and share interactive flow visualizations. Google Services has the capability for multilingual support for over 30 languages and allows the contact center leadership the ability to test and evaluate their contact center agents to uncover any issues that may arise with current processes. Contact Center AI will be used to assist with AI Driven routing to assist with operational efficiency as well as Multimodal and omnichannel customer experience that allows the VA Contact Centers to support Voice Over Internet Protocol (VOIP) via Web Real Time Communication (WebRTC), Chat, and Short Message Service (SMS) traffic.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

The information that is received from the Veterans/Caregivers, VA Employees, and VA Contractors is mainly used to authenticate the individuals on the system. None of the information will be placed in a pre-existing record. The only new record that will be created is anything related to the Call Detail Record (CDR) data that is used to track call quality and length. That data will be available for analytical purposes in CXI. Call centers are open forums where callers may inadvertently disclose personally identifiable information (PII) or protected health information (PHI). To address privacy concerns and regulatory requirements, it is essential to implement robust data management practices for call transcripts. Call transcripts are valuable assets for optimizing agent training, identifying knowledge gaps, and developing new training materials. They can also be used to analyze call trends, agent response times, and call duration to continuously improve the caller experience for Veterans. However, it is crucial to handle these transcripts responsibly, ensuring that personal information is protected and used solely for operational purposes. Veteran Experience Services (VES) and the Unified Communications team is committed to modernizing its call centers and knowledge management processes. Call transcripts will be stored in accordance with existing VA practices and new procedures may be implemented to extract valuable insights for product and program managers.

It is important to note that the primary purpose of analyzing call transcripts is to improve the overall caller experience, not to target individual callers. However, special attention must be paid to callers who are experiencing a mental health crisis. The program leadership is currently evaluating the best approach to handle these cases and in the meantime, we will follow the guidelines established by the call centers and other relevant organizations.

2.3 How the information in the system is 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?
Data in transit: Google protects the integrity of transmitted information by only accepting traffic that conforms to the specification of the network flow policy and by using reliable protocols with error correction to transmit information. External authentication traffic between the user's web browser and Google's application authentication service uses Transport Layer Security (TLS) encryption when users authenticate to their domain. Application layer verification of requests provides additional controls over the confidentiality of transmitted information. External authentication traffic between the user's web browser and Google uses TLS encryption when users authenticate to their domain. Customer core content data is encrypted between customer clients and Google, between Google data centers, and at rest. Encryption between an agency customer and Google servers is dependent on the customer's client configuration.

Data at rest: Google transparently encrypts core content data at rest for user-generated data. Data stored is uniquely labeled and inventoried to allow the file system to identify the location and ownership of end-user data. Data is not stored in a typical file structure but in data "chunks" that are stored on local disks and identified by a unique chunk ID. Google encrypts data as it is written to disk with a unique combination of a per-file encryption key and per end-user Access Control List (ACL) permissions.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).
Google Services uses a Cloud Data Loss Prevention tool that lets customers understand and manage sensitive data. It provides fast, scalable classification, and optional redaction for sensitive data elements such as names, social security numbers, and phone numbers. The Application Programming Interface (API) classifies this data using more than 70 predefined detectors to identify patterns, formats, and checksums, and even understands contextual clues.

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 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Access requirements and roles are documented in accordance with VA Policy. Individuals granted access to PII/PHI adhere to the VA security and privacy listed within VA Handbook 6500 by utilizing approved access control methods such as Account Provisioning Deprovisioning System.

2.4c Does access require manager approval?

Yes, 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?

Yes, access to the PII is being monitored, tracked, or recorded. The Google Security Team uses the following mechanisms to protect the Production network from unauthorized access as well as to ensure the principle of least privilege is implemented at all times. Access control lists (ACLs) protect entry and exit points in the network. These ACLs guarantee that unauthorized entry to the network from the outside world is not permitted and that the management of devices in the network is only possible from within Google's network. A centralized Network Authentication, Authorization, and Accounting (Network AAA) system controls who is authorized to access devices in the network (which segment of the network an engineer may log into), in what capacity (what commands is an engineer permitted to execute when on a device, and which functions he/she has access to), and collects and stores accounting data for auditing and monitoring purposes (e.g. to determine who has done what in the network and to detect intrusions or violations).

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

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
- Full Social Security Number (SSN)
- Partial Social Security Number (SSN)
- Date of Birth
- Mother's Maiden Name
- Personal Mailing Address
- Personal Phone Number
- Personal Fax Number
- Personal Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a Different Individual)
- Financial Information
- Health Insurance Beneficiary Numbers Account Numbers
- Certificate/License Numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Medications
- Medical Records
- Race/Ethnicity
- Medical Record Number
- Tax Identification Number
- Gender/Sex
- Military History/Service Connection
- Next of Kin
- Internal Entry Number (IEN)
- Claim ID
- Patient Internal Control Number (ICN)
- User ID (Unique to Individual)

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

Patient medical records are retained for a total of 75 years after the last episode of care. Department of Veterans Affairs Veteran Health Administration Record Control Schedule (RCS)10-1, Part Three, Chapter Six- Healthcare Records, Item 6000.1a. and 6000.1d.

Office of Information & Technology (OI&T) Records: Destroy when 3 years old or 3 years after applicable agreement expires or is cancelled, as appropriate, but longer retention is authorized if required for business use. These records are created, maintained, and disposed of in accordance with Department of Veterans Affairs, Office of Information & Technology RCS 005-1.

3.3 The retention schedule 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. Please work with the system 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?

Veteran Health Administration: VHA Record Control Schedule 10-1

Veteran Benefit Administration: VB-1 Records Control Schedule

Office of Information Technology: OIT RCS 005-1

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

- Financial Records: Different forms of financial records are retained 1-7 years based on specific retention schedules. Please refer to VHA Record Control Schedule (RCS)10-1, Part Two, Chapter Four- Finance Management

- Patient medical records are retained for a total of 75 years after the last episode of care. VHA Record Control Schedule (RCS)10-1, Part Three, Chapter Six- Healthcare Records, Item 6000.1a. and 6000.1d.

- Office of Information & Technology (OI&T) Records: Mail, printing, and telecommunication services administrative and operational records. These records are created, maintained, and disposed of in accordance with Department of Veterans Affairs, Office of Information & Technology RCS 005-1. Destroy when 3 years old or 3 years after applicable agreement expires or is cancelled, as appropriate, but longer retention is authorized if required for business use. DAA-GRS-2016-0012-0001

- Compensation, pension, and vocational rehabilitation claims folders are retained at the servicing regional office until they are inactive for three years, after which they are transferred to the Records Management.

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.

Google sanitizes media, prior to disposal when released out of organizational control or released for reuse. The Data Destruction Guidelines for Media and the Physical Security Policy outline the policy and guidelines for media sanitization and destruction. Prior to leaving Google's premises, data stored on hard drives are subject to a thorough data sanitization process when disks containing customer information are retired from Google's systems. Google describes its data destruction methods in the Data Destruction Guidelines for Media. Google follows the Clear method recommended by NIST SP 800-88 Rev. 1 "Guidelines for Media Sanitization", Appendix A. First, the disk is logically wiped by authorized individuals. The erasure consists of a full write of the drive with all zeros (0x00) or all ones (0x01) followed by a full read of the drive to help ensure that the drive is blank. These erase results are logged by the drive's serial number for tracking. There is a secondary check before the drives leave the secure facility to ensure the records indicate the media is erased. Finally, the erased drive is released to inventory for reuse and redeployment. Drives that will not be reused are destroyed by shredding the physical drive. The drives do not leave Google control prior to completion of the sanitization process.

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.

Testing: 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.

Research: At this time, no PII/PHI will be used for research purposes.

Training: At this time, no PII/PHI will be used for training purposes.

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 Privacy Officer (PO) 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: *The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.*

Principle of Data Quality and Integrity: *The PIA should describe 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 Google Services 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, the system adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, Google Services will carefully dispose of the data by the determined method as described in question 3.4. Google Services 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 from 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.

PII Mapping of Components

4.1a Google Services consists of one key component (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 Google Services 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 3.9a 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**
Customer Experience Insights (CXI)	Yes	Yes	Internet Protocol (IP) Address Numbers	Receives data from Genesys CX Cloud for call quality and call duration for analytical purposes.	HTTPS / TLS 1.2 Access Control Measures such as PIV Authentication

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Veterans Benefits Administration (VBA) Veterans Benefits Management System (VBMS)	The information is collected from the Veteran for identification and authentication purposes	• Name • Mother's Maiden Name • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Financial Information • Health Insurance Beneficiary Numbers Account Number • Certificate/License Numbers • Military History/Service Connection • Next of Kin • Claim ID	Compensation and Pension Record Interchange (CAPRI) electronic software package
Veterans Health Administration (VHA) Veterans' Health Information Systems and Technology Architecture (VistA)	The information is collected from the Veteran for identification and authentication purposes	• Name • Full Social Security Number • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Emergency Contact Information (Name, Phone Number, etc. of a Different Individual)	Electronically pulled from VistA thru Computerized Patient Record System (CPRS)

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
		• Vehicle License Plate Number • Medications • Medical Records • Race/Ethnicity • Medical Record Number • Gender/Sex • Internal Entry Number (IEN) • Patient Internal Control Number (ICN)	
Office of Information and Technology (OI&T) Login.GOV -e (LG-e)	The information is collected from the Veteran for identification and authentication purposes	• Name • Date of Birth • Full Social Security Number • Partial Social Security Number • Personal Mailing Address • Personal Phone Number(s) • User ID (unique identifier)	HTTPS/443 TLS 1.2
Office of Information and Technology (OI&T) ID.ME -e	The information is collected from the Veteran for identification and authentication purposes	• Name • Date of Birth • Full Social Security Number • Partial Social Security Number • Personal Mailing Address • Personal Phone Number(s) • User ID (unique identifier)	HTTPS/443 TLS 1.2

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in 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, institution, or individual 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 permitted 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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. 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 CX-e, on behalf of JJR Solutions, LLC	The purpose of the information being shared is to assist with authenticating the Veterans /Caregiver as well as assist with providing the responding VA employee with information to assist the Veteran /Caregiver.	• Name • Full Social Security Number • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number • Medical Records • Medications • Military History/Service Connection • Gender/Sex	MOU-ISA (still pending) Business Associate Agreement (BAA)	HTTPS/443 TLS 1.2

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

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

*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, institution, or individual 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 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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

The VHA Notice of Privacy Practice (NOPP) explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non-Veterans receiving care are provided the notice at the time of their encounter.
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

This Privacy Impact Assessment (PIA) also serves as notice As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means. https://department.va.gov/privacy/privacy-impact-assessments/

Privacy notice is provided to veterans via the VA.gov site Privacy Policy page found here: Privacy, Policies, And Legal Information | Veterans Affairs; as well by the Veterans/Caregivers nearest VA Medical Center when they receive care. Notice is also provided in the Federal Register with the publication of the SORN:

23VA10NB3/80FR45590, *Non-VA Fee Basis Records-VA* (7/30/2015)
https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

24VA10A7/85FR62406, *Patient Medical Records-VA* (10/2/2020)
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

34VA10/86FR33015, *Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA* (6/23/2021)
https://www.govinfo.gov/content/pkg/FR-2021-06-23/pdf/2021-13141.pdf

58VA21/22/28/86FR61858, *Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA* (11/8/2021)
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

77VA10E2E/85FR7395, *Health Care Provider Credentialing and Privileging Records-VA* (2/7/2020)
https://www.govinfo.gov/content/pkg/FR-2020-02-07/pdf/2020-02477.pdf

79VA10/85FR84114, *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

89VA10/88FR17639, *Income Verification Records-VA* (3/23/2023)
https://www.govinfo.gov/content/pkg/FR-2023-03-23/pdf/2023-05925.pdf

90VA194/89FR19021, *Call Detail Records-VA* (3/15/2024)
https://www.govinfo.gov/content/pkg/FR-2024-03-15/pdf/2024-05535.pdf

99VA13/74FR14613, *Automated Safety Incident Surveillance and Tracking System-VA* (3/31/2009)
https://www.govinfo.gov/content/pkg/FR-2009-03-31/pdf/E9-7160.pdf

113VA10/88FR32289, *Telephone Service for Clinical Care Records-VA* (5/19/2023)
https://www.govinfo.gov/content/pkg/FR-2023-05-19/pdf/2023-10732.pdf

114VA10/86FR6996, *The Revenue Program Billings and Collection Records-VA* (1/25/2021)
https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf

121VA10/88FR22112, *National Patient Databases-VA* (4/12/2023)
https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

147VA10/86FR46090, *Enrollment and Eligibility Records-VA* (8/17/2021)
https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

168VA005/86FR6975, *Health Information Exchange -VA* (1/25/2021)
https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf

172VA10/86FR72688, *VHA Corporate Data Warehouse-VA* (12/22/2021)
https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf

6.1b If notice was not provided, explain why.

Notice is provided through the various means as outlined in section 6.1a above.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

This Privacy Impact Assessment (PIA) serves as notice of the Google Services 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 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.

Privacy notice is provided to veterans via the VA.gov site Privacy Policy page found here: Privacy, Policies, And Legal Information | Veterans Affairs; as well by the Veterans/Caregivers nearest VA Medical Center when they receive care. Notice is also provided in the Federal Register with the publication of each SORN.

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.

Yes, individuals have the opportunity and right to decline to provide information. However, as this system is dependent upon the individual to share information, this system will be unable to service the individual.

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, an individual's participation on the call is considered to be consenting to VA use of identifier/information.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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

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

<u>Principle of Transparency:</u> This is referring to sufficient notice provided to the individual.

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

<u>Privacy Risk:</u> There is a risk that veterans and other members of the public will not know that the Google Services exists or that it collects, maintains, and/or disseminates PII, PHI or PII/PHI about them.

<u>Mitigation:</u> This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans are enrolled for health care. Additional mitigations are 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 The procedures that allow individuals to gain access to their information.

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

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may *also include additional access provisions.* ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at [VA Public Access Link-Home (efoia-host.com)](https://efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act System of Record Notice. Every Privacy Act System of Record Notice contains information on Contesting Record Procedure which informs the individual who to contact for redress. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA. If any of the information the Veteran provides to authenticate themselves is found inaccurate in their record, they must coordinate with their local VHA Facility to correct that information as it will be used as a means of authentication.

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.

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act System of Records Notice. Every Privacy Act System of Records Notice contains information on Contesting Record Procedure which informs the individual who to contact for redress. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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.

Veterans/Caregivers who need to update information related to benefits that are currently enrolled in the VA Healthcare program can contact their nearest VA Medical Center for assistance with updating their information.

Veterans/Caregivers who are not enrolled in the VA Healthcare program can call 1-900-827-1000 or TTY (Teletypewriter): 711

OIT Records are directly tied the information provided by the system and is real time call detail record data. Information is received directly from the connection between the Veteran/Caregiver and the VA Employee and/or VA contractor so the information would not need to be corrected or have a way to be corrected.

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.

This system does not provide direct access for the Veteran and/or caregiver to correct and update their information. The system uses the information to authenticate the Veterans and Caregivers so that they can be routed correctly and provided information. Access to their medical records and/or benefit records can be coordinated via their local VHA and/or VBA facility.

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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

Principle of Individual Participation: The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their 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. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.

The Notice of Privacy Practices (NOPP) is provided to every enrolled Veteran who receives healthcare 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.

For VA Benefits questions and answers, the Veterans/Caregivers can contact their local VA Medical Center for assistance in gaining access to their information and/or making corrections.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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 Account Provisioning/Deprovisioning System (APDS). Users submit access requests based on need to know and job duties. Supervisor and OI&T approval must be obtained prior to access being 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-user, i.e., Supervisors will have supervisory access and data analytics staff will 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.

VA 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 to 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.

8.2a. Will VA contractors have access to the system and the PII?

Yes, the contractor will receive access to the system once they have received access and have completed all required Privacy and Security training.

8.2b. What involvement will contractors have with the design and maintenance of the system?

Contractors will provide support and recommendation to the Unified Communications team on the design and maintenance of the system.

8.2c. Does the contractor have a signed confidentiality agreement?

The approved contract includes language that the contractor has agreed too as "*Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor may use and disclose VA information only in two situations: (i) in response to a qualifying order of a court of competent jurisdiction after notification to VA Contracting Official (CO) (ii) with written approval from the VA CO. The contractor shall refer all requests for, demands for production of or inquiries about, VA information and information systems to the VA CO for response.*"

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

No, they do not at this time. A BAA will be completed between the vendor and OIT Privacy Office. The Contacting Office, Contracting Officer Representative (COR), and Google will complete the BAA within the 2025 Fiscal Year and prior to official use of the system.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?

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.

No, the contractor does not have a signed non-Disclosure Agreement in place. However, the Contracting Officer Representative (COR) and Contracting Official will review the contract on an annual basis as well as review progress of the actions contracted by the vendor. The contractors will receive access on a "Need to Know" basis that aligns with the VA's Least Privilege model. Contractors will receive a background investigation that is recommended from the Office of Personnel Management (OPM) Position Designation Automated Tool (PDAT). Access to the VA Network is completed via the Account Provisioning/Deprovisioning System (APDS) where they are granted access to security and email groups that they need to have access to. Contractors that require Elevated Privileges (EP) access will receive their access via the VA approved process for assigning Non-Mail Enabled Accounts (NMEA) and access to EP security groups. The contractor is required to ensure that all VA owned information stays within the VA owned systems as well as ensure they protect that information at all times.

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.

Google Services 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 10203: Privacy and HIPPA Training

VA 10204: Privacy and HIPPA Training-Print

VA 20152: Mandatory Training for Transient Clinical Staff

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status:*
2. *The System Security Plan Status Date:*
3. *The Authorization Status:*
4. *The Authorization Date:*
5. *The Authorization Termination Date:*
6. *The Risk Review Completion Date:*
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.***

May 30th, 2025

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. ***(Refer to question 1.8 of the PTA)***

Yes, this system uses cloud technology. Specifically, it uses Google Services (Google Cloud Platform products and underlying Infrastructure) and employs a SaaS cloud model. 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 FR1805751477

9.2 Does the contract with the Hosting 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 3.3.1 of the PTA)* *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes, the VA retains ownership of all VA owned data used within Google Services.

Contract Number: NNG15SD22B
Order Number: 36C10B23F0043
Purchase Order Number: 116S30028

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 not be collected by the Cloud Provider. Ownership of all data will reside with the Department of Veterans Affairs, 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.

Yes, 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 the Department of Veterans Affairs.

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).

Robotic Process Automation (RPA) is used to quickly authenticate the Veteran/Caregiver calling into the VA and route them as quickly as possible to their requested call center and/or contact center.

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: 2025.01.17 08:55:09 -07'00'

Privacy Officer, Julie Drake

JOHN DELEO Digitally signed by JOHN DELEO
Date: 2025.01.17 12:56:04
-05'00'

Information System Security Officer, Martin DeLeo

HARRIS KHAN Digitally signed by HARRIS KHAN
Date: 2025.01.17 14:19:05 -05'00'

Information System Owner, Harris Khan

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).

The VHA Notice of Privacy Practice (NOPP) explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non-Veterans receiving care are provided the notice at the time of their encounter.
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

This Privacy Impact Assessment (PIA) also serves as notice As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.
https://department.va.gov/privacy/privacy-impact-assessments/

Privacy notice is provided to veterans via the VA.gov site Privacy Policy page found here: Privacy, Policies, And Legal Information | Veterans Affairs; as well by the Veterans/Caregivers nearest VA Medical Center when they receive care.

Federal Register with the publication of the following SORNs:

23VA10NB3/80FR45590, *Non-VA Fee Basis Records-VA* (7/30/2015)
https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

24VA10A7/85FR62406, *Patient Medical Records-VA* (10/2/2020)
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

34VA10/86FR33015, *Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA* (6/23/2021)
https://www.govinfo.gov/content/pkg/FR-2021-06-23/pdf/2021-13141.pdf

58VA21/22/28/86FR61858, *Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA* (11/8/2021)
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

77VA10E2E/85FR7395, *Health Care Provider Credentialing and Privileging Records-VA* (2/7/2020)
https://www.govinfo.gov/content/pkg/FR-2020-02-07/pdf/2020-02477.pdf

79VA10/85FR84114, *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

89VA10/88FR17639, *Income Verification Records-VA* (3/23/2023)
https://www.govinfo.gov/content/pkg/FR-2023-03-23/pdf/2023-05925.pdf

90VA194/89FR19021, *Call Detail Records-VA* (3/15/2024)
https://www.govinfo.gov/content/pkg/FR-2024-03-15/pdf/2024-05535.pdf

99VA13/74FR14613, *Automated Safety Incident Surveillance and Tracking System-VA* (3/31/2009)
https://www.govinfo.gov/content/pkg/FR-2009-03-31/pdf/E9-7160.pdf

113VA10/88FR32289, *Telephone Service for Clinical Care Records-VA* (5/19/2023)
https://www.govinfo.gov/content/pkg/FR-2023-05-19/pdf/2023-10732.pdf

114VA10/86FR6996, *The Revenue Program Billings and Collection Records-VA* (1/25/2021)
https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf

121VA10/88FR22112, *National Patient Databases-VA* (4/12/2023)
https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

147VA10/86FR46090, *Enrollment and Eligibility Records-VA* (8/17/2021)
https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

168VA005/86FR6975, *Health Information Exchange -VA* (1/25/2021)
https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf

172VA10/86FR72688, *VHA Corporate Data Warehouse-VA* (12/22/2021)
https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf

Site Type: VHA or Program Office	***Retention Schedule***
VHA	Records Control Schedule 10-1 Records Control Schedule 005-1
VBA	Veterans Benefits-1

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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 Directive 1605.04
IB 10-163p (va.gov)