SPLASH PAGE LANGUAGE

The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

*The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements
under the Federal Information Security Management Act (FISMA).*

VA HANDBOOK 6508: "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 2014, http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=767&FType=2

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Privacy Impact Assessment for the VA IT System called:

Veteran Relationship Management System

VA Center for Innovation Program Office

Date PIA submitted for review:

January 29, 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita K. Grewal	Rita.Grewal@va.gov	202-632-7861
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842-2000 x4613
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-595-7291

Abstract

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

The U.S. Department of Veterans Affairs is building a customer service solution that provides an agent console to better serve and assist calls from Veterans, members of the Armed Forces and family members when they contact the Louis Stokes Cleveland VA Medical Center (abbreviated as VAMC) and VA Community Based Outpatient Clinic (CBOC) Ravenna. They call for a variety of reasons, such as, scheduling appointments, pharmaceutical refills, provider questions, and complaints. The *Veteran Relationship Management System, abbreviated as VRMS* solution is a module built on the Salesforce platform, which is a robust and user-friendly Software as a Service (SaaS) platform.

Veteran Relationship Management System (VRMS) uses the Salesforce Development Platform (SFDP) VA and is hosted in a Federal Risk Authorization Management Program (FedRAMP) certified cloud. The high-level architecture includes a database with an easy to configure "front end" or graphical user interface (GUI) to input and recall information, workflows, reports and dashboards. The functionality includes building integrations to retrieve Veteran information, capturing Veteran preference information, logging call interactions, as well as providing a collaboration tool for informal communication among agents and VAMC leadership. The Salesforce architecture allows developers to create automated processes out of what may have been a pen and paper practice historically.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*

- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?*
- *Does the system use cloud technology? If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.*
- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*
- *NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?*
- *What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

The IT system name is Veteran Relationship Management System (VRMS) and it is owned by VA Center for Innovation Program Office. (*Note: System users decided to change the name of new system from Contact Center Modernization to "Veteran Relationship Management System, abbreviated as VRMS. VRMS and CLE-CCM are synonymous.)*

Salesforce Government Cloud was granted a full ATO by Deputy CIO Service Delivery and Engineering (SD&E), for all applications that sit on the platform. The IT System name is Salesforce Development Platform (SFDP) VA; it is owned by the Office of Information Technology (OI&T), Enterprise Program Management Office (ePMO). The purpose of the IT system is to allow business lines and IT to deliver faster more secure solutions by building on a commercially available Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) product called Salesforce. Salesforce allows the configuration of a graphical user interface (GUI) to provide data entry, workflows, reporting and dashboards. This IT System is categorized as minor and augments a Major Application Salesforce Development Platform (SFDP) VA.

The following Veteran Records will be stored in VRMS

Projected 1-year record additions in Salesforce:	52,416 Veteran records

Salesforce Government Cloud is maintaining underlying physical infrastructure. Additional ISA/MOUs are required between the VA and VA designated contractors/vendors that own the data that is stored or processed within Salesforce Development Platform VA. The vendor-specific agreements will describe the data ownership and storage requirements. The parties agree that transmission, storage and management of VA sensitive information residing in the Salesforce Development Platform VA is the sole responsibility of VA employees or designated contractors/vendors assigned to manage the system. At no time will Salesforce Government Cloud have any access to VA data residing within the Salesforce Development Platform VA. However, Salesforce Government Cloud shall provide the tools to allow VA to properly secure all systems and data hosted in the Salesforce Development Platform VA.

There are two types of users that can manage VRMS data: (1) the authorized module users and based on their permissions they can either create or update the data and (2) VA Salesforce platform Digital Transformation center team.

VRMS is a new module intended to help VA Staff at Medical Centers to respond to veteran calls for patient services, such as scheduling appointments, pharmaceutical refills, provider questions, and complaints. Currently Staff log in to multiple applications to gather information while responding to veteran inquiries. The VRMS module will surface veteran demographic and clinical information in a single place for staff to efficiently respond. Approximately 52,416 Veterans will have their information stored in the VRMS system (for the time period June 2020 - June 2021).

The VRMS application users will ask a Veteran (during an incoming or outbound telephone call) to verbally provide identification information like First Name, Last Name, Social Security Number, Date of Birth so that the users will be able to then conduct a veteran search in the Master Person Index (MPI) system. Identified Veteran demographic information (Name, Social Security Number, Date of Birth, Address, email, veteran service details, and veteran eligibility details) from MPI and Eligibility & Enrollment systems will be retrieved and stored in VRMS.

Veteran Clinical data like Flags, Sensitive Patient, Appointments, Lab results, Allergies, Medications, Notes, Radiology, Medical Problems, Medical Orders, etc. will be retrieved from the Health Data Repository (HDR) system.

Patient care provider individual information such as names, roles and contact phone/pager details will be retrieved from the Patient Centered Management Module (PCMM).

The VRMS module will result in a few business process changes once it is implemented and is being utilized. Part of the project benefit is that it will minimize the number of swivel chair interactions required by the users. By integrating into other source systems that provide demographic and clinical information, the user will be able to see in a single pane what previously would have required swiveling into several systems. In addition, users will leverage the VRMS system to capture call details. This call detail will provide call center management with greater visibility into the reasons Veterans are calling. The call interactions will also assist call center management with resource scheduling.

VRMS Goals

- Create agent console for call center agents to review veteran history and interact with callers
- Verify veteran information using the Master Person Index (MPI)
- Display relevant medical data from Veterans Information Systems, Technology Architecture (VistA), Patient-Aligned Care Team (PACT) and the Computerized Patient Record System (CPRS)
- Track metrics and trends overtime with a customized Dashboard view
- Provide collaboration tool for informal communication among agents and VAMC leadership

VRMS VA Facilities

Personnel from the following VA facilities will use VRMS:

The following is a full list of related laws, regulations and policies and the legal authorities:

- Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317
- Information from the SORN: The Department of Veterans Affairs provides additional notice of this telemedicine system by publishing the following System of Record Notice (SORN):

The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10A7 (Oct. 2, 2020) is available in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104---231, 110 Stat. 3048
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100---503, Computer Matching and Privacy Act of 1988
- E-Government Act of 2002 § 208
- Federal Trade Commission Act § 5
- 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33
- Title 35, Code of Federal Regulations, Chapter XII, Subchapter B
- OMB Circular A---130, Management of Federal Information Resources, 1996
- OMB Memo M---10---23, Guidance for Agency Use of Third---Party Websites
- OMB Memo M---99---18, Privacy Policies on Federal Web Sites
- OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
- OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems"
- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- Federal Information Security Management Act (FISMA) of 2002
- OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- VA Directive and Handbook 6502, Privacy Program
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- State Privacy Laws

The legal authority is 38 U.S.C. 7601-7604 and U.S.C 7681-7683 and Executive Order 9397.

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), *Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.*

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☐ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Account Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Current Medications
☒ Previous Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☒ Other Unique Identifying Number (list below)

Additional SPI: Gender, Date of Death, Preferred Phone Number, Patient ID, Service History, Disability Extremity.

Unique Identifying Number: ICN
The Master Veteran Index ICN is the external ID which is stored on the Contact object in Salesforce. This is the correlation Id between Source system (MPI) and Consumer (Salesforce)

Current Medication and Previous Medical Records:
Flags, Sensitive Patient, Appointments, Lab results, Allergies,
Medications, Notes, Radiology, Medical Problems, Medical Orders, etc. will be retrieved from the Health Data Repository (HDR) system.

PII Mapping of Components

The VRMS system consists of 0 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VRMS and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

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

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

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

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

VRMS receives source information from MPI and HDR. Preference information about the Veteran, is obtained verbally via phone interaction, and may contain PII. The SFDP uses VA Identity and Access Management (IAM) services to validate user login information. The validation of VA employees is done through Active Directory Federated Services (ADFS). Salesforce is hosted in a Salesforce environment within a FedRAMP government certified cloud.

ADFS: All VA employees use their PIV to sign into SFDP using ADFS. This IAM VA service checks the presented A credentials from their PIV card against VA's Active Directory. If an employee is not a user in Active Directory, then they will not have access to SFDP.

MPI: Master Person Index system is the source for Veteran information. MPI is the source of truth for Veteran data and sourced into VRMS salesforce application.

HDR: Health Data Repository is the source system for veteran clinical information in the VRMS module. VRMS doesn't generate any new clinical information in the system, nor does it store or maintain clinical information. Current Medications and Previous Medical records (PHI) are collected from HDR:

- Flags
- Sensitive Patient
- Appointments
- Lab results
- Allergies
- Medications
- Notes
- Radiology
- Medical Problems
- Medical Orders

Veteran: During a veteran phone interaction, VRMS users will collect preference information from the veteran to enhance customer service purposes. Veteran preference information includes:

- Preferred phone number
- Preferred name
- Preferred gender
- Preferred appointment & contact time(s)

PCMM: Patient Centered Management Module (PCMM) provides the Patient care team information (names, role and contact phone numbers).

1.3 How is the information collected?

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

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

The information and data will be collected through validation of the data provided to the team by IAM and their access to the Master Person Index (MPI), the VA Enrollment and Eligibility API (E&E), Patient Centered Management Module (PCMM) and Health Data Repository (HDR) systems. Veteran preference information and Interaction details are manually entered by authorized VRMS users when verbally collected from a Veteran.

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

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

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

The purpose of the veteran information collection is to validate users with Identity and Access Management and collect basic details about the Veteran from the Master Person Index (MPI) and Enrollment & Eligibility (E&E). It is also used to collect veteran clinical data from Health Data Repository (HDR) systems. Data will be encrypted while in transit. The organization is the Office of Information Technology (OI&T).

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

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

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

The VRMS uses MPI database to verify and confirm veteran identity. The VRMS user-interface includes a screen flow for application users to enter first name, last name, social security number and/or date of birth to make a call to the MPI database, verify the identity and pull the veteran information. Subsequently veteran information is saved/updated in Salesforce.

Information in the Master Veteran Index and the Enrollment & Eligibility services is managed by the respective VA units. VRMS is a read-only consumer of this data.

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

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

The following is a full list of related laws, regulations and policies and the legal authorities:

- Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317
- Information from the SORN: The Department of Veterans Affairs provides additional notice of this telemedicine system by publishing the following System of Record Notice (SORN):
    - The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10A7 (Oct. 2, 2020) is available in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf
    -
- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104---231, 110 Stat. 3048
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100---503, Computer Matching and Privacy Act of 1988
- E-Government Act of 2002 § 208
- Federal Trade Commission Act § 5
- 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33
- Title 35, Code of Federal Regulations, Chapter XII, Subchapter B
- OMB Circular A---130, Management of Federal Information Resources, 1996
- OMB Memo M---10---23, Guidance for Agency Use of Third---Party Websites
- OMB Memo M---99---18, Privacy Policies on Federal Web Sites
- OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
- OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems"
- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- Federal Information Security Management Act (FISMA) of 2002
- OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- VA Directive and Handbook 6502, Privacy Program
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- State Privacy Laws

The legal authority is 38 U.S.C. 7601-7604 and U.S.C 7681-7683 and Executive Order 9397.

1.7 <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.

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Sensitive Personal Information (SPI) including personal contact information, SSN and medical information may be released to unauthorized individuals.

Mitigation: Profile based permissions will govern what access users have access to. The profiles will be reviewed on a regular basis to ensure that appropriate information is shared with appropriate users. All employees with access to Veteran's information are required to complete the VA Privacy, Information Security Awareness training and Rules of Behavior annually.

Privacy Risk: Unsecured Sensitive Personal Information (SPI) including personal contact information, SSN and medical information may be exposed.

Mitigation: To mitigate this risk, VRMS protects data by ensuring that only authorized users can access it. Data security rules are assigned that determine which data users can access. All data is encrypted in transfer. Access is governed by strict password security policies. All passwords are stored in Secure Hash Algorithm (SHA) 256 one way hash format.

Privacy Risk: Data breach at the facilities level.

Mitigation: To ensure the utmost privacy and security at the facility level, authorized personnel must pass through multiple levels of biometric and/or badge scanning to reach the salesforce system rooms/cages. All buildings are completely anonymous, with bullet---resistant exterior walls and embassy---grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of a suspected intrusion. Data is backed up. Backups do not physically leave the data center.

Privacy Risk: Data breach at the network level.

Mitigation: Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only https traffic on specific ports, along with Internet Control Message Protocol (ICMP) traffic. Switches ensure that the network complies with the Request for Comment (RFC) 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two---factor authentication, along with the extensive use of technology that controls points of entry.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained.
This question is related to privacy control AP-2, Purpose Specification.

Name: Used to identify the Veteran
Social Security Number: Used as a unique Veteran
Date of Birth: Used to identify Veteran's age
Mailing Address: Used to identify the veteran locations
Gender: Demographic Information
Phone Number: Used for communication
Disability Extremity: Required to provide clinical guidance
Date of Death: Used to identify veteran status when talking to authorized family members
Preferred Phone Number: Required to provide customer service
Veteran Eligibility Status: Used to identify the Veteran Eligibility Status
Current Medications: Required to provide clinical guidance*
Previous Medical Records: Required to provide clinical guidance*
Patient ID: Used to identify the Veteran

Service History: Required to provide customer service
ICN: Used to identify the Veteran
Flags: Required to provide clinical guidance*
Sensitive Patient: Required to provide clinical guidance*
Appointments: Required to provide customer service
Lab results: Required to provide clinical guidance*
Allergies: Required to provide clinical guidance*
Radiology: Required to provide clinical guidance*
Medical Problems: Required to provide clinical guidance*
Medical Orders: Required to provide clinical guidance*

* Realtime APIs in Salesforce were developed to bring the Clinical data from the Health Data Repository system. Through these APIs, VRMS retrieves the current medications and past medications. This data is read only and is not stored in Salesforce. The information is used for VRMS agents, such as nurse triage, to assist a veteran during a phone interaction.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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

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

VRMS does not include tools to perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis.

Salesforce is used to run reports. The system does not create or make available new or previously unutilized information about an individual.

2.3 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. <u>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.</u>

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

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

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

Add answer here:

Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. Access for new users to VRMS are authorized/approved by a VRMS manager. Access requires manager approval. All VRMS access generates system logs in Salesforce. VRMS users follow the same PII/PHI safeguards & VA policies as the applicable to the other systems they use (MPI, HDR, CPRS, etc.). VA and Salesforce have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the Acting Assistant Secretary for information Technology [the VA Designated Accrediting Authority (DAA)].

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
- SSN
- Mailing Address
- Phone Number
- Gender
- Date of Birth
- Date of Death
- Patient ID
- Disability Data
- Service History

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods.

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

Retention of Records is expected to be 75 years. The information is retained following the policies and schedules of VA's Records Management Service and NARA in "Department of Veterans Affairs Records Control Schedule 10-1". Record Control Schedule 10-1 can be found at the following link:
https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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

Directive 6300. Records contained in the Salesforce FedRAMP cloud will be retained as long as the information is needed in accordance with a NARA-approved retention period. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). SFDP records are retained according to Record Control Schedule 10-1. (Disposition of Records) (https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf).

3.4 What are the procedures for the elimination of SPI?

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

Active Data stays on disk until the VA deletes or changes it. Data on backups is retained for 90 days until the backups are overwritten. Log data is retained by Salesforce for a year. VA exports data and retains it to meet VA/NARA retention requirements and dispose of the exported data at the end of the retention period.

When hard drives and backup tapes are at their end of life, the media is sanitized based on Salesforce's Media Disposal Policy. Hard drives are overwritten using a multiple---pass write of complementary and random values. If it wipes successfully, we will return the disk or array to the vendor. If it fails during the wiping process we retain and destroy (i.e., degauss, shred, or incinerate). Backup tapes are degaussed prior to disposal. Specifics on the sanitization process are below.

Salesforce has an established process to sanitize production backup disks and hard drives prior to disposal, release out of salesforce's control, or release to the vendor for reuse. Production backup disks and hard drives are sanitized or destroyed in accordance with salesforce's Media Handling Process. All data is handled and located in VA own Salesforce's servers in Herndon, VA and Chicago, IL in the Salesforce Government Cloud server classification. Said information is handled with proper authority and scrutiny. Hard drives are sanitized within the data center facility using a software utility to perform a seven---pass overwrite of complementary and random values. If the drives wipe successfully, the hardware will be returned to the lessor. If the drive fails during the wiping process the drives are retained within a locked container within the salesforce data center facilities until onsite media destruction takes place. Leasing equipment provides salesforce the opportunity to use the latest equipment available from vendors.

Periodically, a third-party destruction vendor is brought on---site to perform physical destruction of any hard drives that failed overwrite. A certificate of destruction is issued once the media is physically destroyed. Electronic data and files of any type, including PII, Sensitive Personal Information (SPI), and more are destroyed in accordance with the Department of Veterans' Affairs VA Directive 6500 (January 24, 2019), https://www.va.gov/digitalstrategy/docs/VA_Directive_6500_24_Jan_2019.pdf).

When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1. The OIT Chief/CIO will be responsible for identifying and training OIT staff on VA media sanitization policy and procedures. The ISO will coordinate and audit this process and document the audit on an annual basis to ensure compliance with national media sanitization policy.

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

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

PII is not used for research, testing or training.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

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

Follow the format below:

Privacy Risk: The risk to maintaining data within the SFDP is that longer retention times increase the risk that information can be compromised or breached.

Mitigation: To mitigate the risk posed by information retention, the SFDP adheres to the VA RCS schedule for data it maintains. When the retention data is reached for a record, the team will carefully dispose of the data by the determined method as described in question 3.4. All electronic storage media used to store, process, or access VA records will be disposed of in adherence with the latest version of VA Handbook 6500.1, Electronic Media Sanitization.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Master Person Index (MPI)	Verify Veteran Status	● Name ● SSN ● DOB ● Gender ● Phone Number ● Mailing Address ● Facility ID ● Patient ID	Bidirectional system interface via MPI
Eligibility & Enrollments (E&E)	Veteran's Service History and Related Disabilities Informations	● Veteran's Service History ● Veteran's Rated Disability	Salesforce fetches MPI and E&E data as part of a single (VetSearch API) web service. Orchestration handled at DVP layer.
Health Data Repository (HDR)	Provides the Clinical Data of the Veteran	12 different API services are invoked as part of the Clinical data. Here's the list of services: ● Appointments ● Labs ● Vitals ● Radiology ● Flags ● Allergies ● Sensitive Patient Data ● Medical Problems ● Notes ● Medications ● Orders ● Consults	Real time API services are invoked to get the clinical data from HDR services. This data will not be persisted in Salesforce.

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
		Note: Field level details of each API service is not listed here, but can be found in the Technical Design Document (TDD).	
Patient Centered Management Module(PCMM)	Patient-Aligned Care Team information	Names, Contact numbers (Phone, Pager) for the following roles: ● Primary Care Provider ● Care Manager ● Clinical Associate ● Administrative Associate ● PACT Clinical Pharmacist ● Clinical POC ● Administrative POC ● Administrative Associate	Real time web service hosted on Mulesoft Government Cloud from PCMM with Https over SSL/TLS authentication.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Follow the format below:

Privacy Risk: There is a risk that information may be shared with unauthorized VA personnel.

Mitigation: Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training, 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 for the system.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT system*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT system*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*
Salesforce Government Cloud	To store this information in a secure location	PII to include: Name SSN Mailing Address Phone Number Gender Date of Birth Date of Death Patient ID Disability Data Service History	MOU/ISA	Business Extranet Connection (BPE) Connection ID#: B0320

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

<<ADD ANSWER HERE>>

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

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

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

Follow the format below:

Privacy Risk: There is no data being shared outside of the Department. If there is data being shared outside of the department in the future, access controls will be implemented based on MOUs, contracts or agreements.

Mitigation: VA has contracted Salesforce Inc. to deliver services that include maintaining VA data. A contract is in place that clearly articulates Salesforce's roles and responsibilities. Authorized Salesforce personnel access user level data to provision and provide the Salesforce service. Access is controlled by authentication and is restricted to authorized individuals. Salesforce's security policies address the required security controls that must be followed in order to protect PII. Salesforce Development Platform VA will be connected to Equinix for data transfer purposes. The Role of Equinix is to control all the traffic that is going between VA and Salesforce through a designated tunnel. It works as an express gateway and the VA users gets the right bandwidth and less latency in their response from Salesforce. Also, the traffic through this tunnel can be monitored real time by VA network team and if they see any breach they can stop the traffic. Finally, on Salesforce side, there are restrictions to allow traffic that only comes through this tunnel, protecting VA Salesforce Org from any external attacks. Equinix is a network tool in VA IT System to monitor and control traffic between VA and Salesforce cloud. Equinix will provide details of the security event, the potential risk to VA owned sensitive information, and the actions that have been or are being taken to remediate the issue. Activities that will be reported include event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. Equinix will also provide VA with a written closing action report once the security event or incident has been resolved. VA will follow this same notification process should a security event occur within the VA boundary involving Equinix's provided data. Designated POCs will follow established incident response and reporting procedures, determine whether the incident warrants escalation, and comply with established escalation requirements for responding to security incidents.

Section 6. Notice

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

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

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

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

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

The Veteran provides user level data, which may contain PII, for provisioning and providing the salesforce service, and the Customer continues to have access to such information. VA does not otherwise share this information with Salesforce except if required by law to do so. VA has sole ownership of the information and data located in Salesforce's Data Center. VA is the only entity that has access to that said data.

The Department of Veterans Affairs provides notice of this telemedicine system by publishing the following System of Record Notice (SORN):

1. The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10A7 (Oct. 2, 2020) is available in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

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; if a Veteran refuses to provide information suitable for a VRMS agent to search by, they are unable to provide any further assistance to the caller. There is no penalty or denial of service to the veteran.

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

No.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

Follow the format below:
Privacy Risk: There is a risk that VA employees and Veterans will not know that applications built on the SFDP collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

Mitigation: The SFDP Integrated Project Team (IPT) mitigates this risk by ensuring that it provides individuals notice of information collection and notice of the system's existence through the methods discussed in question 6.1. The VA mitigates this risk by providing the public with a form of notice that the system exists, as discussed in detail in question 6.1, including the SORN.

Section 7. Access, Redress, and Correction

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

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

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

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

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

VHA Directive 1605.01 'Privacy and Release Information', section 7(b) states the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request For a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

For preference data stored in the VRMS application, any correction of inaccurate or erroneous information shall be done by the Veteran calling into the call center and verbally providing accurate information. The VRMS user will then make the appropriate update in the VRMS application. VRMS is not the source system of any data other than preference information. Veteran data which is not a preference information will follow the below process for any updates or correction.

Under the jurisdiction of VHA, VHA Directive 1605.01 'Privacy and Release Information', section 8 states the rights of the Veterans to amend their records via submitting VA Form 10-5345a, Individual's Request For a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant or untimely and the reasons for this belief. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy office, or designee, to be date stamped; and to be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579

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 verbally notified that changes can be made for information stored in VRMS but for information where VRMS is not the source system of record below process will be followed.

Notification for correcting the information must be accomplished by informing the individual to whom the record pertains by mail. The individual making the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. The System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee, must notify the relevant persons or organizations that had previously received the record about the amendment. If 38 U.S.C. 7332- protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

VRMS users can update preference information on the Veteran's behalf. If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before, and state that the information they are now providing supersedes that previously provided.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that individuals will be unaware on how to access or correct information in the system.

Mitigation: VRMS Agents are able to correct preference information (Preferred Gender, Preferred Name, Preferred Name etc) in the system if requested. Veterans are verbally notified that changes can be made to their information. Veterans can also find further access, redress, or correction procedures in the source systems PIA.

Section 8. Technical Access and Security

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

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

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

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

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

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

User roles are Agent and Manager. Both have Read/Write access on Case records. The user's role identifies the information and applications a user can access. The distinction between Agent and Manager is controlled by Permission Sets assignments. To receive access to the SFDP, another user of the SFDP with appropriate permissions must sponsor them. The sponsor will describe which applications the user needs to access, the user's role, and any security caveats that apply to the user. These roles will be governed by permission sets that allow field level contract of the information and data. This information is documented in the user provisioning process with the Digital Transformation Center.

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

The contractors who provide support to the system are required to complete annual VA Privacy and information Security and Rules of Behavior training via the VA's Talent Management System (TMS). The Office of Contract Review operates under a reimbursable agreement with VA's Office of Acquisition, Logistics and Construction (OALC) to provide pre-award, post-award, and other requested reviews of vendors' proposals and contracts. Contractually all contractors are required to sign the VA Form 0752 NDA.

System Owner and Contracting Officer Representative (COR) is the individual to accept and amend any incoming or outgoing contracts involving Salesforce Development Platform VA.

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.

Initial and annual Security Awareness Training includes security best practices, threat recognition, privacy, compliance and policy requirements, and reporting obligations. Upon completion of training, personnel must complete a security and privacy quiz with a passing score. All required VA privacy training must be completed in TMS prior to the user being provisioned.

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

If Yes, provide:

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

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

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

The Salesforce Development Platform VA last ATO was issued on 6/5/2019. It is set to expire 12/31/2023. The SFDP categorization is Moderate.

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2021.02.25 23:02:25 -05'00'

Privacy Officer, Rita Grewal

James C. Boring 149438

Digitally signed by James C. Boring 149438
Date: 2021.02.25 09:13:56 -05'00'

Information Security Systems Officer, James Boring

Michael S. Domanski 326889

Digitally signed by Michael S. Domanski 326889
Date: 2021.02.25 08:42:49 -05'00'

Information System Owner, Michael Domanski

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).