Privacy Impact Assessment for the VA IT System called:

Salesforce- VA Customer Experience Services Recovery Platform

Veteran Affairs Central Office (VACO)

Veteran Experience Services (VES)

eMASS ID # 2035

Date PIA submitted for review:

10/11/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Gina Siefert	Gina.Siefert@va.gov, OITPrivacy@va.gov	202-632-8430
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842-2000 x4613
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-482-1398

Abstract

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

The Salesforce-VA Customer Experience Service Recovery Platform (VA CX SRP) application is used by Veterans, their family members, and other concerned parties to request assistance with VA programs and benefits. The VA CX SRP software is used by two call centers known as VA Hotline and Tier 1, as well as five Office of Client Relations (OCR) teams from Veterans Benefits Administration (VBA), Veterans Health Administration (VHA), Office of Secretary VA (OSVA), Board of Veterans Appeals (BVA), and the National Cemetery Administration (NCA). General inquiries, questions about identity theft, and VA.gov helpdesk assistance are received by Tier 1 (MyVA411). Inquiries about complex or sensitive topics are taken by VA Hotline agents and referred to the OCR teams at VBA, VHA, OSVA, BVA, and NCA. There are approximately 410 VA CX SRP users of which 320 are call center agents. The call centers are administered by Veterans Experience Office (VEO) Operations located in Salt Lake City, Utah (Tier 1), and Shepherdstown, West Virginia (VA Hotline). The VA CX SRP case tracking system runs on VA's Salesforce platform and provides end-to-end call management features, including case, complaint, and account management, role, and team-based auto-assignment, and knowledgebase features. The system can handle a range of document attachments, with cascading picklists and access to other time-saving functions, such as real time case status, Service Level Agreement (SLA) compliance, email-to-case, web-to-case, chat, and survey request capabilities. The system incorporates S-docs for Salesforce – a document generation and storage, e-signature app from Salesforce AppExchange. The VA CX SRP is integrated with ID.me and the Master Person Index - Enhanced (MPI-e). VA CX SRP was formerly known as the White House VA Hotline (WHHL). The name was changed effective November 1, 2022.

VA CX SRP is located on the VA Main organization.

Overview

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

1 *General Description*

A. *What is the IT system name and the name of the program office that owns the IT system?*
Salesforce- VA Customer Experience Service Recovery Platform is a Salesforce software application that is owned by the Office of Information Technology (OIT).

B. *What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*
The VA CX SRP is operated under the auspices of Veteran Experience Office (VEO) program. VA CX SRP project aims to provide VA employees who communicate with Veterans, family members, and members of the public a single desktop view with consistent and up-to-date information, as well as rapid and accurate issue resolution. The VA CX SRP application utilizes Salesforce software application as the base of its functionality and is hosted in the Salesforce Government Cloud.

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

VA CX SRP is owned by the Office of Information Technology (OI&T) Development, Security, and Operations (DevSecOps) Product Engineering (PE), Enterprise Program Management Office (EPMO), Veteran Experience Services (VES), Veteran Relationship Management (VRM) Product Line.

2. Information Collection and Sharing

D. *What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?*

Since the inception of the VA CX SRP application in 2017, through the writing of this document, interactions for 9,444,391 unique named patients (i.e., excluding anonymous interactions) have been entered in VA CX SRP. Patients for which VA CX SRP stores information can Veterans, non-Veterans and VA Employees (including contractors).

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

The VA CX SRP application captures Interactions with Veterans, beneficiaries, advocates, and even members of the public. VA CX SRP Contact Center Agents and Office of Client Relations (OCR) Team Members can also leverage real-time Veteran feedback for effective service recovery. Feedback entered into the application is received through multiple channels (both internal and external to the VA), such phone calls or voicemails, emails, letters, and other systems. Cases are routed and tracked through resolution. Additionally, VHA Concern, Recommendation, and Compliment case types are sent to Office of Patient Advocacy (OPA) Patient Advocates through an integration with the Patient Advocate Tracking System (PATS-R). After the cases are resolved in PATS-R, activities and resolution information are updated on cases in VA CX SRP.

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

VA CX SRP – VA Systems Inventory (VASI) #2620 – has interfaces to several other internal VA systems. VA CX SRP displays but does not retain (unless entered into the Interaction by the Contact Center Agents / OCR Team Members) data from the following VA Systems:

System Name	**VASI**
Master Patient Index (MPI)	#1406
Patient Advocate Tracking System Replacement (PATS-R)	#2402
VA Profile	#2203
Summit Data Platform (SDP) Customer Experience Data Warehouse (CxDW)	#2266

G. *Is 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?*

VA CX SRP is a cloud-based software application, hosted on the Salesforce Government Cloud, that is utilized by two call centers (VA Hotline, and Tier 1), as well as five OCR teams from VBA, VHA, OSVA, BVA, and the NCA. As a cloud-based application, all software boundaries and security controls are identical, and management of PII remains consistent for all application users regardless of their physical location.

3. Legal Authority and SORN

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

The VA CX SRP application has legal authority to operate the following federal regulations and/or departmental policies and guidelines, as follows:

- Authority for maintenance of the system: Title 38, United States Code, Chapter 73, section 7301(b).
- Title 38, United States Code, Section 501-Veterans' Benefits.
- Join Commission National Patient Safety Goals- Goal 1: Improve the accuracy of patient identification.
- VHA Directive 1906- Data Quality Requirements for Healthcare Identity Management and the Master Veterans Index Functions.
- VHA Directive 2009-021 Data Entry Requirements for Administrative Data.
- VHA Directive 2006-036 Data Quality Requirements for Identity Management and the Master Patient Index Functions.
- VHA Directive 2007-037 Identity Authentication for Health Care Services.
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000.
- VA Directive 6300, Records, and Information Management.
- VA Handbook 6500, VA6500 AC-8: System Use Notification.
- The Privacy Act of 1974.
- 147VA10 / 86 FR 46090; "Enrollment and Eligibility Records-VA" (August 17, 2021).
- 121VA10 / 83 FR 6094; "National Patient Databases-VA" (April 12, 2023).

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

VA CX SRP falls under System of Records Notices (SORNs) "147VA10 / 86 FR 46090", and "121VA10 / 83 FR 6094". These SORNs are up-to-date and address the use of cloud technology. More information provided in Section 6.1 below.

4. System Changes

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

No. The completion of this PIA is not expected to result in changes to business processes.

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

No. The completion of this PIA is not expected to result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☒ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☒ Gender
☒ Integrated Control Number (ICN)
☐ Military History/Service Connection
☒ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements: Electronic Data Interchange Personal Identifier (EDIPI), Preferred Mailing Address, Appeals ID, MPI External ID same as Internal Control Number (ICN), VA Email Address, Work Phone Number, Work Mailing Address, Username (same as VA email), Alias (short name used to identify user), Federated ID (same as username and VA email), Government email address.

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

PII Mapping of Components (Servers/Database)

VA CX SRP 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 **VA CX SRP** and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

- Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**Does this system collect PII? (Yes/ No)**	**Does this system store PII? (Yes/ No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
Salesforce – VA Customer Experience Service Recovery Platform	Yes	Yes	• Date of Birth (DoB) • MPI External ID (same as ICN) • Social Security Number (SSN) • Name • Personal Email Address • Personal Phone Number • Cell Phone Number • Personal Fax Number • Next of Kin • Personal Address (residential) • Preferred Mailing Address • Gender • Date of Death • Claim Number • Electronic Data Interchange Personal Identifier (EDIPI) • VA Email Address • Work Phone • Work Mailing Address • Username (same as VA email)	• Identification • Identification • Identification • Identification • Communication • Communication • Communication • Communication • Communication • Communication • Communication • Communication • Communication • Communication • Communication • Communication • Communication • Communication • Communication	Encrypted electronic transmission (web service)

			• Alias (short name used to identify user) • Federated ID (same as username and VA email) • Appeals ID	• Communication • Communication • Identification	

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

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

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

The Sources of Information for the VACX SRP application are as follows:
- Caller interaction/confirmation
- MPI
- Integrated VHA Systems, including PATS-R

The primary source of information in the VA CX SRP application is direct interaction/ confirmation via telephone communication with Contact Center Agents. Other sources of information are received by the Office of Client Relations teams through email, telephone, and letters. Callers provide at least three (3) identification factors for the Veteran (first name, last name, Date of Birth (DoB), Social Security Number (SSN)) to search MPI. MPI returns basic personal data about a Veteran (name, SSN, address, etc.).

Source	Description
Caller Interaction	Information from the caller is recorded in Salesforce. Information from other systems can be confirmed by caller interaction.
MPI	At least three factors provided by the Caller (First Name, Last Name, DoB, SSN) are used to search MPI. MPI returns Veteran data which is stored in CRM as part of the Veteran's Record. The Veteran's Integration Control Number (ICN) is also returned by MPI and is stored by Salesforce.
PATS-R	An integration is available between PATS_R and VA CX SRP so VA CX SRP users will not have to email or create dual entries for the same patient need.

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.

Information pulled from sources above is used to ensure Call Center Agent / OCR Team Members receive all information necessary to create the interaction. Information is verified during the interaction.

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

Based on the interactions with the caller, the Contact Center Agent/OCR Team Member's create Cases. Cases can contain information about the interaction recorded on the Salesforce Case Notes field.

1.3 How is the information collected?

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

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

Information used in the VA CX SRP application is collected from Veterans, Veteran family members, and advocates over the phone and entered into the system by a Contact Center Agent or OCR Team Member. The Contact Center Agent or OCR Team Member may conduct a search against MPI, which returns a Veteran's name, SSN, ICN and other details.

During the Contact Center Agent/OCR Team Member's interaction with the caller, the Contact Center Agent/OCR Team Member may discover that additional actions outside of their purview are required to resolve a caller's inquiry. As such, they can make an annotation in the Salesforce Case Notes field and forward the case record to a colleague in a different VA Administration across the department, such as Debt Management, for follow-up.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

The information collected by VA CX SRP is not collected on a form subject to the Paperwork Reduction Act.

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

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

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

Veteran identity is checked for accuracy through MPI. Callers must provide at least three (3) identifiers for the Contact Center Agent/OCR Team Member to conduct a successful

MPI search. This ensures that the correct Veteran or Beneficiary is associated to a Request. Personal information from the Veteran is then populated into the Request form and Veteran Record. The Contact Center Agent/OCR Team Member verifies with the Veteran or Beneficiary whether their information is correct. MPI is the authoritative source to validate a Veteran or Beneficiary. The Contact Center Agent/OCR Team Member cannot directly change the information from the authoritative source within VA CX SRP.

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?

All integrated VA systems perform their own data validation processes. The VA CX SRP application relies on the integrated source systems (NPI, PATS-R, VA Profile and CxI) listed in Table 4.1 below) to provide data; VA CX SRP does not run extra validation; it only displays the data from the source systems. Therefore, it is assumed the data has already been validated prior to its collection and usage. VA CX SRP is an interface application, information/data update happens in the source application per their policy and procedures.

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

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

The VA CX SRP application complies with the following federal regulations and/or departmental policies and guidelines, as follows:

- Authority for maintenance of the system: Title 38, United States Code, Chapter 73, section 7301(b).
- Title 38, United States Code, Section 501-Veterans' Benefits.
- Join Commission National Patient Safety Goals- Goal 1: Improve the accuracy of patient identification.
- VHA Directive 1906- Data Quality Requirements for Healthcare Identity Management and the Master Veterans Index Functions.
- VHA Directive 2009-021 Data Entry Requirements for Administrative Data.
- VHA Directive 2006-036 Data Quality Requirements for Identity Management and the Master Patient Index Functions.
- VHA Directive 2007-037 Identity Authentication for Health Care Services.
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000.
- VA Directive 6300, Records and Information Management.
- VA Handbook 6500, VA6500 AC-8: System Use Notification.

- The Privacy Act of 1974.

SSN and DOB are used to verify, through MPI, the identity of Veterans to be able to research the Veteran's file. The legal authority is as follows:

- VA SORN #147VA10NF1, Enrollment and Eligibility Records—VA (August 17, 2021)
- VA SORN #121VA10A7, National Patient Databases—VA (April 12, 2023).

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Caller (i.e., Veteran, Beneficiary, or Provider) may provide incorrect identity information.

Mitigation: Veteran information is validated through MPI, as the authoritative source for identity, before call proceeds and any historical information is provided. Additional information gathered and provided is based on MPI-returned identifiers. The Contact Center Agent / OCR Team Member does not provide PII from the errant MPI search to the caller as a means of selecting the correct Veteran or Beneficiary.

Privacy Risk: Contact Center Agent/OCR Team Member may enter caller-provided information erroneously.
Mitigation: Veteran information is validated through MPI, as the authoritative source, before any information is provided. Additional information gathered and provided is based on MPI-returned identifiers. The Contact Center Agent/OCR Team Member will be aware of incorrectly

entered data because the MPI search will return zero records or the MPI results will return a Veteran, Beneficiary, or a Beneficiary's sponsor (Veteran) who is not the subject of the call.

Privacy Risk: Data pulled by the VA CX SRP application contains PII. If the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft might result.
Mitigation: The VA CX SRP application ensures strict access to information by enforcing thorough access control and requirements for end users. Access to the application is by PIV authentication. Individual administrator user IDs and access are provided based on need. The Call Center limits access rights and controls only to valid end users. There are rigorous securities monitoring controls to prevent unauthorized access and intrusion, and to protect all information. Furthermore, all end users are required to take VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203) training annually. All users with access to VA CX SRP are responsible in assuring safeguards for the PII.

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 correctly identify and search criteria to located case(s) within VA Salesforce. Used to map data transfers from MPI to VA Salesforce.	Not used externally
Date of Birth (DoB)	Identification	Not used externally
Date of Death	Identification	Not used externally
Personal Address (residential)	Identification/Communication	Not used externally
Preferred Mailing Address	Identification/Communication	Not used externally
Social Security Number (SSN)	Identification	Not used externally
MPI External ID (same as ICN)	Identification	Not used externally
Personal Email Address	Communication	Not used externally
Personal Phone Number	Communication	Not used externally
Personal Fax Number	Communication	Not used externally
Next of Kin	Communication	Not used externally
Gender	Identification	Not used externally

Claim Number	Determine Benefit Support	Not used externally
Electronic Data Interchange Personal Identifier (EDIPI)	Determine Benefit Support	Not used externally
VA Email Address	Communication	Not used externally
Work Phone Number	Communication	Not used externally
Work Mailing Address	Communication	Not used externally
Username (same as VA email)	Communication	Not used externally
Alias (short name used to identify user)	Communication	Not used externally
Federated ID (same as username and VA email)	Identification/Communication	Not used externally
Appeals ID	Identification	Not used externally

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

These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

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

The Salesforce platform (which VA CX SRP is built on) provides out-of-the-box reporting capabilities which can provide analysis and reports of data housed in the system. The data analysis capabilities of Salesforce Platform allow users to generate configurable reports on an ad-hoc or scheduled basis. These reports consist of a summary data that lists the number of records that meet various criteria, and basic analysis including call resolution totals and percentages. There is no reporting on Veterans or Beneficiaries, or their inquiries.

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.

VA CX SRP does not create or make available any new or previously unutilized clinical or benefits information about any individual. VA CX SRP does, however, record interaction details between the agent and customer. These details may include free-form notes and comments about the customer service issue.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

The following measures are in place to protect VA CX SRP data while in transit and at rest VA Network (Firewall), PIV authentication via native integration with VA Active Directory (AD), Salesforce out-of-the-box encryption, and Salesforce Shield Encryption. All VA CX SRP users are VA employees or contractors that have been granted VA accounts contingent on completed the VA's background check and onboarding process.

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

Supplementary security has been built into the VA CX SRP to encrypt SSN fields.

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

PII and PHI within the VA CX SRP application is safeguarded behind the following: VA Network (Firewall), PIV authentication via native integration with VA Active Directory (AD), Salesforce out-of-the-box encryption, and Salesforce Shield Encryption. Additionally, the VA CX SRP application ATO is certified as MODERATE and is hosted under a Cloud Services Provider (CSP) ATO that is FedRAMP certified with a National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 199 Security Classification of HIGH.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

The SORN defines the information use of the information and how the information is accessed, contained, and stored in the system. As per the SORN, strict control measures are enforced to ensure that access to and disclosure are limited to a need-to-know based on official duties. Access to the computerized information is limited by means of passwords and authorized user identification codes.

The VA CX SRP application is accessible by both VA employees and contractors who require logical access to VA information services/applications. Account creation is managed and offered through VA via two factor authentication (2FA) Personal Identity Verification (PIV) card. Native integration with the VA Active Directory (AD) is used to provide credential access to VA modules/communities residing in the Salesforce application, the determinant of access is organizational affiliation rather than personal identity. For some module(s) the required organizational e-mail confirmation and multi-factor authentication (MFA) will be enforced (IAL1), but no identity proofing (IAL2) and vice versa.

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

Yes, 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, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. 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 Authorizing Official (AO)]. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how Veterans' information is used, stored, and protected.

2.4c Does access require manager approval?

Yes, managers must approve any new users accessing the system. Access requests go through many layers of approvals. Salesforce software licenses cannot be issued without manager approval. Managers will reject any applications from individuals who do not work with them, do not require access, or are not using the correct e-mail address.

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

The VA CX SRP application implements auditing which tracks user access to the system and all data accessed. Audit log records are created and maintained in the application.

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

VA ensure that the practices stated in the PIA are reinforced by requiring Contractors and VA employees to complete all VA trainings including VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and Health Insurance Portability and Accountability Act (HIPAA) Training (VA 10203). Contractors and VA employees are required to agree to all rules and regulations outlined in trainings, along with any consequences that may arise if failure to comply. Ultimately, safeguarding PII and PHI is a core VA objective and is everyone’s responsibility.

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*

Listed below is the only information retained in the VA CX SRP application:

- Name
- Social Security Number (SSN)
- Date of Birth (DOB)
- Date of Death
- Personal Address (Residential)
- Preferred Mailing Address
- Personal Phone Number(s)
- Personal Email Address
- Personal Fax Number
- MPI External ID
- Gender
- Next of Kin
- Claim Number
- Appeals ID
- Electronic Data Interchange Personal Identifier (EDIPI)
- VA/Government Email Address
- Work Phone Number
- Work Mailing Address
- Username (same as VA Email)
- Alias (Short name used to identify user)
- Federated ID (same as username and VA email)

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

VA will retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA) approved record retention schedule. OIT retains audit records for a defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and VA information retention requirements. minimum of 1 year or as documented in the NARA retention periods, HIPAA legislation (for VHA), or whichever is greater. Audit logs which describe a security breach must be maintained for 6 years (HIPAA requirement).
Link to NARA within RCS 10-1: 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)?

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

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

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

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

Salesforce Government Cloud Plus complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6500. Records contained in the Salesforce FedRAMP cloud will be retained if 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). SFGCP records are retained according to the Record Control Schedule 10-1 Section 4 (Disposition of Records). Request for Records Disposition Authority. Disposition Authority: DAA-0015-2013-0004.
Link to RCS 10-1: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

3.4 What are the procedures for the elimination or transfer of SPI?

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

VA CX SRP follows VA Directive 6500.
https://www.va.gov/vapubs/search_action.cfm?dType=1

All electronic storage media used to store, process, or access records will be disposed of in adherence with this directive. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. In the event data extension is unused for six (6) months, then the cloud-hosted regulations, Salesforce Data Retention Policy will be implemented as needed. Salesforce Government Cloud Plus commits to removing data entirely from their systems within six (6) months after archiving/end of contract.

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

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

No PII/live data is used for training, testing, or research. All training materials display example data using test Veterans. All internal employees with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

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

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

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

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

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

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

Follow the format below:

Privacy Risk: If information is retained longer than specified, privacy information may be released to unauthorized individuals.

Mitigation: The risk associated with the length of time the data is retained is considered minimal. All data at rest within the VA CX SRP security boundary is encrypted in accordance with FIPS 140-2, as well as protected by FEDRAMP certified "Moderate" security controls. Use of FedRAMP Moderate controls implemented under the FedRAMP ATO. Collectively, these controls within the VA CX SRP security boundary provide maximum protection to all VA Salesforce data. VA CX SRP only retains the required relevant information relevant as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA) approved record retention schedule.

Privacy Risk: If Veteran data is lost in a disaster scenario prior to being backed up, then full indefinite retention of data will not be achieved.

Mitigation: All primary production servers are backed up on a daily incremental and weekly full basis employing Salesforce native backup/restore capabilities with the data stored in geo-redundant Government data centers.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

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

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

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

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

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

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Master Patient Index (MPI)	Veteran identity confirmation and return of system identifiers	Name; Date of Birth; SSN; EDIPI	Encrypted electronic transmission (web service)
Patient Advocate Tracking System Replacement (PATS-R)	Provides Veterans inquiries, complaints, and compliments	Name; Date of Birth; SSN; EDIPI	Encrypted electronic transmission (web service)
VA Profile	Provides Veteran/Beneficiary contact information	Name; Personal Address (residential); Preferred Mailing Address; Personal Email Address; Personal Phone Number; Work Phone Number and Cell Phone Number	Encrypted electronic transmission (web service)
Customer Experience Insights (CxI) formerly Customer Experience Data Warehouse (CxDW)	Data extracts created for reporting purposes	Name; Personal Address (residential); Preferred Mailing Address; Personal Email Address; Personal Phone Number; Work Phone Number and Cell Phone Number, Date of Birth; MPI External ID; SSN; Personal Fax Number; Next of Kin; Gender; Date of Death; Claim Number; Appeals ID; EDIPI	Encrypted electronic transmission (web service)
Global Access Locator (GAL)	Identification	Name, Work Phone Number	Encrypted electronic transmission (web service)
Salesforce AppExchange	Management of documentation (digital signature)	No PII/PHI data elements will be shared/visible	Encrypted electronic

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Application S-docs for FOIA			transmission (web service)
Salesforce Lighthouse API Platform	Confirmation of veteran addresses	Name, Personal Address (Residential); Preferred Mailing Address	Encrypted electronic transmission (web service)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: If appropriate safeguards are not in place, then Privacy information shared within the Department may result in unauthorized data access.

Mitigation: The VA CX SRP application ensures strict access to information by enforcing through access control and requirements for end users. Access to the application is by PIV authentication. Individual administrator user IDs and access are provided only based on need. VA CX SRP limits access rights and controls only to valid end users. Rigorous security monitoring controls are in place to prevent unauthorized access and intrusion, and to protect all information. Furthermore, all end users are required to take VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203) training annually. The VA IT office is responsible in assuring safeguards for the PII. Note, data is transmitted via secure connection to Salesforce. MPI keeps records of which users search for which individuals; Modules do not keep logs as this would require permanently storing data, which modules do not do, for privacy reasons.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: VA CX SRP does not share any data that is being held in the system. Therefore, no privacy risks are associated with sharing information outside of the VA.

Mitigation: There is no information being shared externally and no privacy risks associated with data sharing; therefore, the mitigation strategy is not applicable.

Section 6. Notice

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

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

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

All callers are informed via the IVR that each call is being recorded. Call Center Agents are trained to utilize guidelines established by Routine Use 27 (RU27) which describe 27 different routine use categories allowing for the collection of information that is released to different agencies or persons for different reasons.

1. The two SORNs applicable to the system provide notice of collection of information.
   The SORNs covering the VA CX SRP application are as follows:
   • 147VA10 / 86 FR 46090; "Enrollment and Eligibility Records-VA" (August 17, 2021)
   https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf
   • 121VA10 / 83 FR 6094; "National Patient Databases-VA" (April 12, 2023)
   https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf.
   Posted privacy policy, Privacy Act statements are published via SORN in the Federal Register at: https://www.oprm.va.gov/privacy/systems_of_records.aspx.

2. This Privacy Impact Assessment (PIA) also serves as a notice of this system.
3. Additionally, all callers are informed via the Interactive Voice Recognition (IVR) that each call is being recorded, and that that their PII will be used to resolve the subject for which they are calling.

The VA policy is not to disclose any personal information to third parties outside VA without their consent, except to facilitate the transaction, to act on caller's behalf at their request, or as authorized by law. Any questions or concerns regarding VA privacy policy or use of caller's information can be made by contacting via email at Contact VA Privacy Service, or by mailing questions or concerns at Department of Veterans Affairs, Privacy Service, 810 Vermont Avenue, N.W. (005R1A) Washington, DC 20420. This Privacy Impact Assessment will be available online as required by the Government Act of 2002, Pub. L. 107–347§208(b)(1)(B)(iii). More detail on privacy policy can be found at VA Privacy Policy at https://www.va.gov/privacy/.

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

Notice was provided as described in response to 6.1a. Applicable SORNs are posted on the Federal Register, and VA Privacy Policy is available online. Additionally, all callers are informed via the Interactive Voice Recognition (IVR) that each call is being recorded, and that that their PII will be used to resolve the subject for which they are calling.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

All callers are informed via the IVR that each call is being recorded. Call Center Agents are trained to utilize guidelines established by Routine Use 27 (RU27) which describe 27 different routine use categories allowing for the collection of information that is released to different agencies or persons for different reasons.

All calls are recorded and may be monitored for quality assurance. Call Center Agents collect information directly from Veterans, Beneficiaries, and Providers. If the caller asks, notice of what information is required is provided at the time of the call. Providers or Beneficiaries must provide at least three (3) identifiers in order for the Call Center Agents to conduct an MPI search. This ensures that the correct Beneficiary is associated to a phone call record being created in Call Center Agents. Personal information from the Veteran or Beneficiary is then populated into the phone call form. The Call Center Agents can then verify with the caller whether the information is correct. The VA CX SRP application logs all interactions that the Veteran, Beneficiary, or Provider has with the Call Center, the reasons for the contact, and how the Call Center supported the caller. PII, including SSN, DOB, and names, can be saved as part of the call log.

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.

VHA Handbook 1605.01 'Privacy and Release Information', Section 5 a. (8) lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually- identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

Veterans have the right to refuse to disclose their SSNs to VHA. The individual is denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (please refer to the: 38 Code of Federal Regulations CFR 1.575(a)). If a caller does not wish to provide their SSN, they may provide their First Name, Last Name, and Date of Birth. If the caller does not wish to provide any of this information, there is no denial of service; however, the Contact Center Agent will be unable to 1) Create a request in Salesforce to be routed to another user to work on; and 2) Effectively categorize the call type and details. Inability to perform these actions may restrict or prevent the Call Center Agent's ability to assist the caller.

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.

VHA Handbook 1605.1, Appendix D: Privacy and Release Information, Section 5 lists the rights of the Veteran to request that the VHA restrict the use and/or disclosure a person's individually identifiable health information to carry out treatment, payment, or health care operations. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility maintaining the record.

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

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

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

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: If Call Center Agents do not provide notice to callers, then they will not know how the information they provide to VACX SRP is being used. The magnitude of impact is low if Veterans and Beneficiaries are not provided this notice because the Call Center Agents are not collecting new data.
Mitigation: The SF-VACX SPR Team 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 two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Act statement and the SORNs..

Section 7. Access, Redress, and Correction

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

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

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

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

As VA CX SRP is not a formal system of record, there are no processes for correcting inaccurate information. Inaccuracies must be corrected within the authoritative source systems of record, Enrollment & Eligibility or National Patient Database SORN states:

Individuals seeking information regarding access to and contesting of Enrollment and Eligibility Records may write to the Director, Health Eligibility Center, 2957 Clairmont Road, Atlanta, GA 30329 as directed in the Enrollment and Eligibility Records-VA (147VA10) SORN, available at:

https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

Individuals seeking information regarding access to and contesting of National Patient Databases incorrect information or wishing to obtain more information about access, redress, and record correction should contact the Department of Veterans Affairs regional as directed in the National Patient Databases-VA (121VA10 / 83 FR 6094) SORN, available at: https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

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

The system is not exempt from the 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?

As VA CX SRP is not a formal system of record, there are no processes for correcting inaccurate information. Inaccuracies must be corrected within the authoritative source systems of record, Enrollment & Eligibility or National Patient Database. Please see response to Question 7.1a.

Individuals seeking information regarding access to and contesting of Enrollment and Eligibility Records may write to the Director, Health Eligibility Center, 2957 Clairmont Road, Atlanta, GA 30329 as directed in the Enrollment and Eligibility Records-VA (147VA10) SORN, available at: https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

Individuals seeking information regarding access to and contesting of National Patient Databases incorrect information or wishing to obtain more information about access, redress, and record correction should contact the Department of Veterans Affairs regional as directed in the National Patient Databases-VA (121VA10 / 83 FR 6094) SORN, available at: https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

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.

As VA CX SRP is not a formal system of record, there are no processes for correcting inaccurate information. Inaccuracies must be corrected within the authoritative source systems of record, Enrollment & Eligibility or National Patient Database.

Individuals seeking information regarding access to and contesting of Enrollment and Eligibility Records may write to the Director, Health Eligibility Center, 2957 Clairmont Road, Atlanta, GA 30329 as directed in the Enrollment and Eligibility Records-VA (147VA10) SORN, available at: https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

Individuals seeking information regarding access to and contesting of National Patient Databases incorrect information or wishing to obtain more information about access, redress, and record correction should contact the Department of Veterans Affairs regional as directed in the National Patient Databases-VA (121VA10 / 83 FR 6094) SORN, available at: https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

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.

As VA CX SRP is not a formal system of record, there are no processes for correcting inaccurate information. Inaccuracies must be corrected within the authoritative systems of record, including Enrollment & Eligibility or National Patient Database.

Individuals seeking information regarding access to and contesting of Enrollment and Eligibility Records may write to the Director, Health Eligibility Center, 2957 Clairmont Road, Atlanta, GA 30329 as directed in the Enrollment and Eligibility Records-VA (147VA10) SORN, available at: https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

Individuals seeking information regarding access to and contesting of National Patient Databases incorrect information or wishing to obtain more information about access, redress, and record correction should contact the Department of Veterans Affairs regional as directed in the National Patient Databases-VA (121VA10 / 83 FR 6094) SORN, available at: https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

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.

Formal redress is provided, so no alternatives are necessary.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

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

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

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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:

<u>Privacy Risk:</u> There is a risk that data contained within the various source systems is incorrect and individuals could be unaware of access, redress, and correction procedures.

<u>Mitigation:</u> No personal data is collected directly from individuals. Information is gathered from various source systems. The PIA and the SORNS from the source systems are available to be referenced as needed. These publicly available documents would cover the information access procedures.

Section 8. Technical Access and Security

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

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

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

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

The VA CS SRP platform is accessible to both VA Employees and contractors who require logical access to VA information services. Account creation is managed and offered through VA via two factor authentication (2FA) Personal Identity Verification (PIV) card and native integration to the VA Active Directory (AD). VA CX SRP will NOT allow users to perform any actions without appropriate identification and/or authentication. Internal/platform users must complete VA's OI&T On-boarding process and obtain a VA email address before a user account can be provisioned/permission in VA Salesforce platform.

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?

Not Applicable. Individuals from other agencies do not have access to VA CX SRP.

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.

Following user Provisioning (as implemented for VA Salesforce Community) access to information and applications components is governed by Permission Sets and assignment to user groups. Permission sets allow for field level control of information and data. To receive access to VA CX SRP another current system user with appropriate permissions must sponsor that person. The sponsor will describe which functionality the user needs to access, the user's intended function, and any security caveats that apply to the user. There are six main functional roles (sometimes referred to as user roles), as well as functional roles for each of the five OCR teams. The VA CX SRP business users classify themselves by these functional roles; they are as follows:

1. Contact Center Agent
2. Contact Center Supervisor
3. Veterans Experience Office (VEO) Operations (Management).
4. VA.gov Technical Support Team.
5. Enterprise Veterans Self Service (EVSS) Technical Support Team.
6. Freedom of Information Act (FOIA) Officer.
7. Office of the Secretary of the VA (OSVA) Office of Client Relations.
8. Veterans Benefits Administration (VBA) Office of Client Relations.
9. Veterans Health Administration (VHA) Office of Patient Advocacy (OPA) Operations.
10. National Cemetery Administration (NCA) Office of Client Relations.
11. Board of Veterans Appeals (BVA) Office of Client Relations.

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

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

The VA Contract Officer’s Representative (COR) for the Salesforce DTC contract along with the VA Salesforce System Owner maintain governing authority over all VA Salesforce environments. The Salesforce DTC team will maintain users, update applications and components, introduce new functionality, govern deployment activities, and ensure user operability. The Salesforce DTC members, are not primary users, will monitor and reviews VA Salesforce related support contracts on a regular basis to ensure no gaps in support for the application its users. Developers do not have access to production PII. The Salesforce Digital Transformation Center (DTC) contractor team supports the VA Salesforce production environment and as such has access to the VA Salesforce system and data contained therein. This includes PII and VA Sensitive Information. The following steps are required before contractors can gain access to the system:

- Contractors must take and pass training on VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203), and government ethics and role-based training based on support role to the system.
- Contractors must have signed the Non-Disclosure Agreement (NDA) and Rules of Behavior (RoB).
- Contractors must have successfully completed VA contractor background security investigation as per the Position Designation Automated Tool (PDT).
- Once complete, a request is submitted for access. Before access is granted to the production environment; this request must be approved by the supervisor, and OIT.

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.

Personnel who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Information Security Rules of Behavior (RoB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA’s TMS. After the WHHL user’s initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. This training includes, but is not limited to, the following TMS Courses:

- VA 10176: Privacy and Info Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training
- VA 3812493: Annual Government Ethics

Role-based Training Includes, but is not limited to and based on the role of the user:

- VA 1016925: Information Assurance for Software Developers IT Software Developers.
- VA 1357084: Information Security Role-Based Training for Data Managers.
- VA 64899: Information Security Role-Based Training for IT Project Managers.
- VA 3197: Information Security Role-Based Training for IT Specialists.
- VA 1357083: Information Security Role-Based Training for Network Administrators.
- VA 1357076: Information Security Role-Based Training for System Administrators.
- VA 3867207: Information Security Role-Based Training for System Owners.

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

8.4a If Yes, provide:

1. *The Security Plan Status: Approved*
2. *The System Security Plan Status Date: 26 June 2023*
3. *The Authorization Status: Approved (Minor applications receive and approval)*
4. *The Authorization Date: 26 June 2023*
5. *The Authorization Termination Date:26 June 2026*
6. *The Risk Review Completion Date: 12 March 2021*
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.***

Not applicable.

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

The VA CX SRP application is a commercially available Platform-as-a- Service (PaaS) and Software-as-a-Service (SaaS) product. The Salesforce Government Cloud Plus ATO maintains the underlying physical infrastructure for VA CX SRP and other Salesforce applications in use in the VA. The Salesforce Government Cloud Plus Cloud Service Provider (CSP) is Amazon Web Services (AWS). VA CX SRP System utilizes Salesforce Gov Cloud Plus. Salesforce

Government Cloud Plus is hosted in the AWS GovCloud. The Salesforce Government Cloud Plus (SFGCP-E) is built on the underlying Salesforce Force.com that is hosted in a FedRAMP Certified FISMA High environment which is in the Amazon Web Services (AWS) GovCloud West. This software utilizes the PaaS Service of Salesforce Gov Cloud Plus. The system is housed in Government Cloud on the FedRAMP-authorized Salesforce Government Cloud Plus (SFGCP).

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes, VA has full ownership of the PII/PHI that will be shared through SF VCL. Contract agreement "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B, Order Number: 36C10B23F0172, Expiration Date: June 25, 2025.

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.

The VA CX SRP, CSP, and Salesforce contracts establish VA ownership rights of all data including PII. The contracts stipulate that the contractor shall not retain any copies of data, in full or in part, at the completion of the performance period. The data shall contain no proprietary elements that would preclude the VA from migrating the data to a different hosting environment or from using a different case management system in the future.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

The Salesforce contract addresses the National Institute of Standards (NIST) 800-144 principle that states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf."

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).

RPAs are not utilized.

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.

GINA SIEFERT Digitally signed by GINA SIEFERT
Date: 2024.10.30 11:45:14 -05'00'

Privacy Officer, Gina Siefert

JAMES BORING Digitally signed by JAMES BORING
Date: 2024.10.30 15:12:25 -04'00'

Information System Security Officer, James Boring

MICHAEL DOMANSKI Digitally signed by MICHAEL DOMANSKI
Date: 2024.10.30 14:58:00 -04'00'

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; screen shot of a website collection privacy notice).

The SORNs covering the VA CX SRP application are as follows:
- 147VA10 / 86 FR 46090; “Enrollment and Eligibility Records-VA” (August 17, 2021) https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf
- 121VA10 / 83 FR 6094; “National Patient Databases-VA” (April 12, 2023) https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

More detail on privacy policy can be found at VA Privacy Policy at https://www.va.gov/privacy.

Government Act of 2002, Pub. L. 107–347§208(b)(1)(B)(iii).

VHA Handbook 1605.1, Appendix D: Privacy and Release Information, Section 5

HELPFUL LINKS:

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

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

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

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices