Privacy Impact Assessment for the VA IT System called:

Salesforce – Integrated Ethics Web (IEWeb)

Veterans Health Administration

National Center for Ethics in HealthCare

eMASS ID #1894

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	Joseph Facciolli	Joseph.Facciolli@va.gov	215-842-2000X4613
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 for VA?".

Salesforce- Integrated Ethics Web is a cloud software development system that VA is using to migrate legacy systems and technologies including Microsoft Access and SharePoint. The system is hosted on the Salesforce Government Cloud Plus-Enterprise (SFGCP-E) Platform which 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 workflows for approvals and quality assurance steps for online documents. 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 Privacy Impact Assessment (PIA). A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 *General Description*

A. *What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*
Salesforce - Integrated Web Ethics (IE Web), National Center for Ethics in Health Care (12ETH). It helps to:
• Manage the complex ethics consultation process
• Add functionality for ethics activity logging
• Provide new functionality for preventive ethics consultation management
• Provide flexible search and reporting capabilities

B. *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*
The system is hosted on Salesforce Government Cloud Plus-Enterprise Platform. It is VA Controlled / non-VA Owned.

2. Information Collection and Sharing

C. *Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*
Information is collected for each consult entered into the system. There is typically one or two individuals whose information is entered into the system per consult. The typical client is an inpatient Veteran. It is also common for Veteran Caregivers or surrogates to enter a consult. Currently, we expect about 300,000-400,000 individuals whose information will be stored in the system.

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

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

Salesforce- Integrated Ethics Web, which is a branch of the Salesforce Government Cloud Plus (SFGCP) was granted a full ATO by Deputy CIO Service Delivery and Engineering (SD&E), for all applications that sit on the platform. The umbrella IT System name is Salesforce Government Cloud Plus; 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. Currently, we expect about 300,000-400,000 individuals whose information will be stored in the system. This is a system that is hosted in a FedRAMP certified government cloud. It will not fall under a region.

Salesforce Government Cloud Plus (SFGCP) 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 Government Cloud Plus (SFGCP). 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 Government Cloud Plus (SFGCP) is the sole responsibility of VA employees or designated contractors/vendors assigned to manage the system. At no time will Salesforce Government Cloud Plus (SFGCP) have any access to VA data residing within the Salesforce Government Cloud Plus (SFGCP). Thus, all agreements on data and system responsibilities shall not be covered in this base agreement (MOU). However, Salesforce Government Cloud Plus (SFGCP) shall provide the tools to allow VA to properly secure all systems and data hosted in the Salesforce Government Cloud Plus (SFGCP).

The goal of this initiative is for the National Center for Ethics in Health Care (NCEHC) to be able to manage the Ethics Consultations (EC) Ethics Activity Log (EAL) & Preventive Ethics (PE) in Salesforce Government Cloud Plus (SFGCP) and to provide a better user experience. The Salesforce - Integrated Web Ethics (IE Web) Application will help to:

- Manage the complex ethics consultation process
- Add functionality for ethics activity logging
- Provide new functionality for preventive ethics consultation management
- Provide flexible search and reporting capabilities

E. *What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.*
Information is contained in the system. No sharing.

F. Are the modules/subsystems only applicable if information is shared?
No, the information stays within the system

G. *Is the system operated in more than one site to include primary and secondary site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?*
The system is used enterprise-wide and the same controls are in place at all sites.

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

H. *What is the citation of the legal authority and SORN to operate the IT system?*
Title 38, U.S.C., 501(b), 304, 7301, and 7304(a).

I. *What is the SORN?*
152VA10 “Integrated Ethics Web Database (IEWeb)—VA”, https://www.govinfo.gov/content/pkg/FR-2021-11-30/pdf/2021-26026.pdf. Authority for maintenance of the system: Title 38, U.S.C., 501(b), 304, 7301, and 7304(a).

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

4. System Changes

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

☐ *Yes* ☒ *No*

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

☐ *Yes* ☒ *No*

Section 1. Characterization of the Information

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

1.1 Information collected, used, disseminated, created, or maintained in the system.

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

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

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

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

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

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

Other PII/PHI data elements: Consultation Narrative, Medical Notes, Ethics Rating, Age, Case Description, Activity Description, Major Cause.

1.2 List the sources of the information in the system

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

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

The Salesforce- IEWeb uses two 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) and Veterans' information is validated using Access VA and their internal resources. Salesforce - IEWeb is hosted in a Salesforce environment within a FedRAMP government certified cloud.

ADFS: All VA employees use their PIV to sign into Salesforce 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 Salesforce Government Cloud Plus-E platform.

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.

AccessVA: AccessVA is utilized in the credential validation process as well as assisting in the creation of a Single Sign-On external capability. Applications using IAM's AccessVA allow access, and use the application via accepted AccessVA credentials. The information from AccessVA is required because it is the VA system that allows single sign-on access and VA prefers that application utilize this single sign-on functionality.

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

It generates Salesforce reports only.

1.3 Methods of information collection

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

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

The information and data will be collected through validation of the data provided to the team by IAM and their access to the Master Veteran Index (MVI).

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?
Not applicable. No form associated.

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

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

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

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?
No, the system does not

1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.

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

SORN 152VA10 "Integrated Ethics Web Database (IEWeb)—VA", https://www.govinfo.gov/content/pkg/FR-2021-11-30/pdf/2021-26026.pdf. Authority for maintenance of the system: Title 38, U.S.C., 501(b), 304, 7301, and 7304(a).

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: *The collection ties with the purpose of the underlying mission of the organization and its enabling authority.*

Principle of Minimization: *The information is directly relevant and necessary to accomplish the specific purposes of the program.*

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

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

Follow the format below when entering your risk assessment:

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

Mitigation: Depending on level of authority granted to the respective user by their home department via the VA, each user will have sensitivity level of access to veteran data based on profile-based permissions. 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, SFDP 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: There may be a 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 ports 80 and 443, 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 that will be used in support of the program's business purpose.

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

PII/PHI Data Element	Internal Use	External Use
Name	Used to Identify Veteran	Not used
SSN	SSN or last 4 of SSN used as patient identifier reference	Not used
Phone Number	Used for communication	Not used
Consultation Narrative	Information to be documented	Not used
Medical Notes	additional useful information	Not used
Ethics Rating	Required for Record	Not used
Age	demographic	Not used
Sex	demographic	Not used
Case Description	Required for record should include ethics concern	Not used
Activity Description	Required for record	Not used
Major Cause	Required for record. Strategies need to be proposed to address each cause.	Not used

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

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

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.*

It does not create new information

2.3 How the information in the system is secured.

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

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

Controls, including encryption, 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 Designated Accrediting Authority (DAA)].

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

Controls, including encryption, 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 Designated Accrediting Authority (DAA)].

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

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 Designated Accrediting Authority (DAA)].

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

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

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

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

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

2.4a How is access to the PII determined?

Users must be appointed by a facility and approved by a VACO regional team member verifying that access is warranted.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

VHA Directive 1004 – VHA Health Care Ethics defines ethics consultants and team members. These individuals require access to Salesforce – Integrated Web Ethics (IEWeb).

2.4c Does access require manager approval? Yes, access requires a manager's approval.

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

Yes, access is tracked via Salesforce platform.

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

VHA Office of Information and Technology ensures the following 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 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 • Phone Number • Consultation Narrative • Notes • Ethics Rating • Age • Sex • Case Description • Activity Description • Major Cause

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*
All system records maintained outside the Electronic Health Record will be maintained in accordance with General Records Schedule (GRS) 2.8 Ethics Program Records Item 010 as identified in SORN 152VA10.
RCS 10-1: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

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

3.3a Are all records stored within the system of record indicated on an approved disposition authority?
Salesforce – IEWeb complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records contained in the Government Cloud Plus (SFGCP) will be retained as long as the information is needed in accordance with a NARA-approved retention period. The records are kept under the disposition authority outlined in SORN 152VA10. https://www.govinfo.gov/content/pkg/FR-2021-11-30/pdf/2021-26026.pdf.

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

Salesforce-IEWeb complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records contained in the Government Cloud Plus-

Enterprise platform (SFGCP-E) will be retained as long as the information is needed in accordance with a NARA-approved retention period.
Per SORN 152VA10, Records that are stored within Computerized Patient Record System (CPRS) and Veterans Health Information Systems and Technology Architecture (VistA) will be maintained in accordance with Record Control Schedule (RCS) 10–1 Item 6000.2, Electronic Health Records, NARA job# N1–15–02–3. https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf. All other records maintained outside the Electronic Health Record will be maintained in accordance with General Records Schedule (GRS) 2.8 Ethics Program Records Item 010 with disposition authority DAA-GRS-2016-0006-0001. https://www.archives.gov/files/records-mgmt/grs/grs02-8.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.
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 Government Cloud Plus-Enterprise (SFGCP-E) for a year. VA exports data and retain 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 Plus (SFGCP) 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 with 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?

PII is not used for research, testing or training – rather a “scrubbed” subset of data or “dummy” data may be used.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

Principle of Minimization: *The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.*

Principle of Data Quality and Integrity: *The PIA should describe policies and procedures for how PII that is no longer relevant and necessary is purged.*

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

Follow the format below:

Privacy Risk: 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 schedules for each category or 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.

PII Mapping of Components

4.1a Salesforce – Integrated Ethics Web (IEWeb) consists of 2 key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Salesforce – Integrated Ethics Web (IEWeb) and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A	N/A	N/A	N/A	N/A	N/A

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

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

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

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

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

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

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

Data Shared with Internal Organizations

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
This program is used by the National Center for Ethics in Health Care (NCEHC) facility staff and VHACO staff.	To manage documentation for Ethics Consultations (EC) and Ethics Activity Logs (EAL) in Salesforce and to provide a better user experience	Name, SSN, Work/Personal Phone Number, Work/Personal Email, Fax Number, Consultation Narrative, Medical Notes, Ethics Rating, Age, Sex, Case Description, Activity Description, Major Cause	Users are granted permissions to the Salesforce platform via the Salesforce DTC team. All access requests are verified and approved by National Center for Ethics in Health Care staff.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions in this section.).
This question is related to privacy control UL-1, Internal Use.
Follow the format below:
Privacy Risk: 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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

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

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

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

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

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

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

Data Shared with External Organizations

List IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
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: No information is shared outside of the VA.

Mitigation: No information is shared outside of the VA.

Section 6. Notice

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

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

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

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

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

Notice is also provided in the Federal Register with the publication of the SORN 152VA10, https://www.govinfo.gov/content/pkg/FR-2021-11-30/pdf/2021-26026.pdf.

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

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.

Salesforce's Master Subscription Agreement addresses the protection of Customer Data. A sample Master Subscription Agreement can be viewed at http://www.salesforce.com/assets/pdf/misc/salesforce_MSA.pdf. In addition to the Master Subscription Agreement, Salesforce has documented a System Security Plan that identifies the security controls that Salesforce has documented to protect the environment in which Customer Data is stored. Additionally, their privacy and security statements can be viewed at http://www.salesforce.com/company/privacy. Salesforce has a Global Privacy Team who oversees privacy for salesforce. Protecting the security and privacy of user data is a shared responsibility between Salesforce and VA that provision user accounts, as stated in the Salesforce Security Guide (https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/salesforce_security_guide.htm).

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

6.1b If notice was not provided, explain why.
Notice was provided as described in 6.1a above.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.
Notice was provided as described in 6.1a above.

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.
Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them. 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)).

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.
Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR. Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.
Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: This is referring to sufficient notice provided to the individual.

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

Privacy Risk: There is a risk that Veterans and VA employees who use the system will not know that Salesforce - IEWeb, collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

Mitigation: The Salesforce- IEWeb 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 two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Act statement and the SORN 152VA10.

Section 7. Access, Redress, and Correction

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

7.1 The procedures that allow individuals to gain access to their information.

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

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

As specified in SORN 152VA10, individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA healthcare facility location where they are or were employed or made contact or they may write to the National Center for Ethics in Health Care at 810 Vermont Avenue NW, Washington, DC 20420. https://www.govinfo.gov/content/pkg/FR-2021-11-30/pdf/2021-26026.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 Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?
The information in this system is maintained under Privacy Act SORN 152VA10.

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

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.
Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A.

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

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.
Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) which states:

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

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

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

As specified in SORN 152VA10, individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA healthcare facility location where they are or were employed or made contact or they may write to the National Center for Ethics in Health Care at 810 Vermont Avenue NW, Washington, DC 20420.
https://www.govinfo.gov/content/pkg/FR-2021-11-30/pdf/2021-26026.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 via the amendment process is available to all individuals, as stated in questions 7.1-7.3.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

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

Mitigation: The risk of incorrect information in an individual's records is mitigated by authenticating information when possible. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.
The NOPP discusses the process for requesting an amendment to one's records.

The Release of Information (ROI) office is available at the VA facility where they receive treatment to assist Veterans with obtaining access to their health records and other records containing personal information.

As specified in SORN 152VA10, individuals seeking information regarding access to and contesting of records in this system may also write to the National Center for Ethics in Health Care at 810 Vermont Avenue NW, Washington, DC 20420.

Section 8. Technical Access and Security

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

8.1 The procedures in place to determine which users may access the system, must be documented.

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

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

User roles identify the information and applications a user can access. To receive access to the Salesforce - IEWeb, 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.

8.1b 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?
Users from other agencies do not have access.

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.
Admin., member, or read only access.

8.2a. Will VA contractors have access to the system and the PII?
Yes, they will have access if they are granted access to the system and have the correct permissions.

8.2b. What involvement will contractors have with the design and maintenance of the system?
Salesforce Direct To Customer provides all maintenance of the system including addressing trouble tickets.

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

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.

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

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

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

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.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 8/3/2022
3. *The Authorization Status:* ATO
4. *The Authorization Date:* 6/26/2023
5. *The Authorization Termination Date:* 6/26/2026
6. *The Risk Review Completion Date:* 06/26/2023
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.***

This does not apply.

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. ***(Refer to question 1.8 of the PTA)***

Salesforce- Integrated Ethics Web is hosted on the platform Salesforce Government Cloud Plus-Enterprise, which is a FedRAMP approved platform. 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 workflows for approvals and quality assurance steps for online documents. The Salesforce architecture allows developers to create automated processes out of what may have been a pen and paper practice historically.

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.1 of the PTA)* *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

VA has control/operates this system

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

No, it will not

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.

We are not the owners of the large salesforce contract.

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).

This system does not use RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

PHILLIP CAUTHERS

Digitally signed by PHILLIP CAUTHERS
Date: 2025.05.20 12:20:40 -04'00'

Privacy Officer, Phillip Cauthers

JOSEPH FACCIOLLI

Digitally signed by JOSEPH FACCIOLLI
Date: 2025.05.21 09:54:02 -04'00'

Information System Security Officer, Joseph Facciolli

MICHAEL DOMANSKI

Digitally signed by MICHAEL DOMANSKI
Date: 2025.05.22 11:09:46 -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).

VA Notice of Privacy Practices
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

SORN 152VA10, Integrated Ethics Web Database (IEWeb)-VA
https://www.govinfo.gov/content/pkg/FR-2021-11-30/pdf/2021-26026.pdf

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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

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

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

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

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
VA Notice of Privacy Practices