Privacy Impact Assessment for the VA IT System called:

Salesforce Development Platform (SFDP) White House VA Hotline (WHHL)

Benefits, Appeals, and Memorials (BAM)Veteran Relationship Management

Date PIA submitted for review:

September 29, 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	*Rita Grewal*	*Rita.Grewal@va.gov*	*202-632-7861*
Information System Security Officer (ISSO)	*James Boring*	*James.Boring@va.gov*	*215-842-2000 x4613*
Information System Owner	*Michael Domanski*	*Michael.Domanski@va.gov*	*202-461-9825*

Abstract

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

The White House / VA Hotline (WHHL) is a Salesforce software application that supports the Department of Veterans Affairs Tier 1 and the White House VA Hotline Contact Centers, as well as Office of Client Relations stakeholders representing the Office of the Secretary of Veterans Affairs (OSVA), Veterans Benefits Administration (VBA), Veterans Health Administration (VHA), National Cemetery Administration (NCA), and Board of Veterans' Appeals (BVA). The application enables 350+ users to answer general information queries, address VA.gov issues, provide directory assistance, and navigate to the right subject matter expert for Veterans, family members, and beneficiaries. It also provides a tool to intake, and track (through resolution) concerns routed downstream to VA administration OCR teams and other personnel involved in the complaint management process in the field and in program offices. In October 2017, VA established a dedicated hotline where calls are answered by a live agent 24/7/365. The contact center, which is supported by an operations team located across the country and two physical locations, Shepherdstown, WV and a second site in Salt Lake City, UT (opened in October 2019), is staffed with just under 300 people.

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

An overview of the WHHL provided as follows:
The White House / VA Hotline is a Salesforce software application that is owned in collaboration between Veterans Affairs Central Office (VACO) Information Technology Support Services (ITSS), Access Management/VA Business Module Owners and Office of Information Technology (OIT).

The WHHL project falls under the Veteran Experience Office (VEO) program. The WHHL project aims to provide VA employees who communicate with Veterans, family members, and the general public a single desktop view with consistent and up-to-date information, as well as rapid and accurate issue resolution. The WHHL application utilizes Salesforce software application as the base of its functionality and is hosted in the Salesforce Government Cloud.

The WHHL application captures Interactions with Veterans, beneficiaries, advocates, and even the general public. WHHL Contact Center Agents can also leverage real-time Veteran feedback for effective service recovery. Feedback entered into the WHHL 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.

In addition, VHA Concern, Recommendation, and Compliment case types are sent to 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 WHHL.

WHHL collects, and stores caller information needed to resolve caller requests, including first and last name, address, phone number, emails, Social Security Number (SSN), and Date of Birth (DOB).

The WHHL application utilizes web services from the

- Master Patient Index (MPI) to confirm Veteran identity and obtain corresponding identifiers for other systems.
- IAM - SSOi Integration for Single Sign-On and authentication
- Patient Advocate Tracking System-Replacement (PATS-R)

The WHHL application is not a regional General Support System (GSS), Veterans Health Information Systems and Technology Architecture (VistA), or Local Area Network (LAN), and does not provide direct support to hospitals/medical centers or other regional offices.

The WHHL application has legal authority to operate under “Title 38, United States Code, Section 501 – Veterans’ Benefits” and SORNs”, “147VA10NF1”, and “121VA10P2”. More information provided in Section 1.6 below.

The completion of this PIA is not expected to result in circumstances that will require changes to business processes or technology used.

Section 1. Characterization of the Information

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

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

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

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

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

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

Additional Information Collected:

- Case Subject
- Case Number
- Case Notes
- MPI External ID
- Gender
- Next of Kin
- Date of Death
- Claim Number
- Appeals ID
- Appeals Description
- Appeals Date
- Appeals Location
- Appeals Agency of Original Jurisdiction

PII Mapping of Components

WHHL consists of **4** key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by WHHL and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Interaction	Yes	Yes	Name, SSN, DOB, Phone Number(s), Fax Number, EDIPI	Caller identification. Veteran identity verification	Access to system is limited; access requires PIV; access to system and components is audited
Request	Yes	Yes	Name, SSN, DOB, Phone Number(s), Fax Number, EDIPI	Veteran identity verification; Customer service (retrieval of claims, appointments, consults, notes)	Access to system is limited; access requires PIV; access to system and components is audited
Contact Object (Veteran and Non-Veteran)	Yes	Yes	Name, SSN, DOB, Phone Number(s), EDIPI	Veteran identity verification; Customer service (retrieval of claims, appointments, consults, notes)	Access to system is limited; access requires PIV; access to system and components is audited
Case Notes Field	Yes	Yes	Name, SSN, DOB, Mother's maiden name, Address, zip code, Phone Number, email address	To correct erroneous information, update information, or complete missing information	Free form text that is entered into Notes is stored in the Salesforce database that is hosted in a FISMA Moderate environment.

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

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

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

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

The Sources of Information for the WHHL application are as follows:

- Caller interaction/confirmation
- MPI
- Integrated VHA Systems, including PATS-R

The primary source of information in the WHHL 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, DoB, 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 WHHL so WHHL users will not have to email or create dual entries for the same patient need.

1.3 How is the information collected?

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

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

Information used in the WHHL application is collected from Veterans, Veteran family members, and advocates over the phone and entered into the system by a Contact Center Agent or Office of Client Relations (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.

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

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

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

Veteran identity is checked for accuracy through MPI. Callers must provide at least three (3) identifiers in order 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 Salesforce.

All integrated VA systems perform their own data validation processes. The WHHL application relies on the integrated systems to provide data and so therefore WHHL does not run extra validation and only displays the data from the external systems. Therefore, it is assumed the data has already been validated prior to its collection and usage.

WHHL 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 WHHL application complies with the following federal regulations and/or departmental policies and guidelines, as follows:

- 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 in order to be able to research the Veteran's file. The legal authority is as follows:

•VA SORN#147VA10NF1, Enrollment and Eligibility Records—VA
•VA SORN#121VA10A7, National Patient Databases—VA (121VA10P2)

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

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

<u>Principle of Minimization:</u> 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.

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 WHHL 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 WHHL 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 WHHL 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 will be used in support of the program's business purpose.

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

- Name – Used to correctly identify and search criteria to located case(s) within VASalesforce. Use to map data transfers from MPI to VA Salesforce.
- Date of Birth - Used to correctly identify user/Veteran
- Date of Death - Used to correctly identify user/VeteranMailing Address – Used to correctly identify user/Veteran.
- Social Security Number – Used to correctly identify user/Veteran.
- Phone Number – Used to correctly identify user/Veteran.
- Personal Fax Number – Used to correctly identify user/Veteran.
- Email Address – Used to correctly identify user/Veteran.
- MPI External ID - Used to correctly identify user/Veteran.
- Gender – Use to complete Veteran's profile.
- Next of Kin: Used in cases of emergent situations such as medical emergencies. Used when patient expires and in cases of patient incapacity.
- Case Subject- Used to determine benefit support
- Case Number - Used to determine benefit support
- Case Notes - Used to determine benefit support
- Claim Number - Used to determine benefit support
- Appeals ID - Used to determine benefit support
- Appeals Description - Used to determine benefit support
- Appeals Date - Used to determine benefit support
- Appeals Location - Used to determine benefit support
- Appeals Agency of Original Jurisdiction - Used to determine benefit support

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

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

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

Salesforce 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.
WHHL does not create or make available any new or previously un-utilized clinical or benefits information about any individual. WHHL does 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?

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

The following measures are in place to protect WHHL data while in transit and at rest:

- VA Network (Firewall),
- PIV,
- Salesforce out of the box encryption,
- Salesforce Shield Encryption

In addition, SSN fields in WHHL are encrypted at the field level.

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

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

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

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

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

Add answer here:

The Salesforce FedRAMP MODERATE ATO package employs security controls in the respective MODERATE security control baselines unless specific exceptions have been allowed based on the tailoring guidance provided in VA agency moderate ATO for Salesforce and NIST Special Publication 800-53 and specific VA directives.

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 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.

Access Control:
The VA SF platform is accessible to both internal and external users 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 and/or AccessVA. Single Sign On external (SSOe) 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. The 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. IAM systems verify credential and collect audit logs based on access requested and may contain PII that might have been captured into order to authenticate to the resource.

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

The information listed below is the only information retained in the WHHL database:

- Full Name
- Social Security Number (SSN)
- Date of Birth (DOB)
- Date of DeathMailing Address
- Zip Code
- Phone Number(s)

- Email Address
- Personal Fax Number.
- MPI External ID
- Gender
- Next of Kin
- Case Subject
- Case Number
- Case Notes
- Claim Number
- Appeals ID
- Appeals Description
- Appeals Date
- Appeals Location
- Appeals Agency of Original Jurisdiction

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

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

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. A 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).

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

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

Information is retained as determined by the VA Business Module Owner and/or community partners who oversee and maintain these collaborations.

This system complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records contained in the Salesforce FedRAMP cloud will be retained as long as the information is needed in accordance with a NARA-approved retention period. SFDP records are retained according to Record Control Schedule 10-1 (reference: https://www.archives.gov/files/recordsmgmt/grs/grs04-1.pdf

3.4 What are the procedures for the elimination of SPI?

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

SFDP follows VA Handbook 6300.1, "Records Management Procedures. Electronic data and files of any type, including PII, PHI, SPI and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Media Sanitization (January 23, 2019). 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 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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

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.

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

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

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

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

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

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

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 SFDP 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 SFDP security boundary provide maximum protection to all VA Salesforce data. SFDP 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 via 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 3.10 (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 shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Master Patient Index (MPI)	Veteran identity confirmation and return of system identifiers	Shared: • First Name • Last Name • DOB • SSN • EDIPI	Encrypted electronic transmission (web service)
Patient Advocate Tracking System Replacement	Provides Veterans inquiries, complaints, and compliments	Shared: • First Name • Last Name • DOB • SSN • EDIPI • Case Notes	Encrypted electronic transmission (web service)
VA Profile (Read-only)	Provides Veteran/Beneficiary contact information	Shared: • Address • Email address • Phone	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.
This question is related to privacy control UL-1, Internal Use.

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

Mitigation: The WHHL 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. WHHL 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 3.11 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 shared/received with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

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

The WHHL application does not share information with external organizations; therefore, no specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16.

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.

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

Privacy Risk: WHHL 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 notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

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

The 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/. Posted privacy policy, Privacy Act statements are published via SORN in the Federal Register https://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf.

All callers are informed via the Interactive Voice Recognition (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 release of information 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 WHHL 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 Directive 1605.1 Appendix D 'Privacy and Release Information', Section 5 lists the rights of Veterans and Beneficiaries to request VA to restrict the use and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations. 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:

- Create a request in Salesforce to be routed to another user to work on
- 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 of the individual'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 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: If Call Center Agents do not provide notice to callers, then they will not know how the information they provide to the WHHL 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: Contractor and VA employees 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. In addition, this PIA, which will be available online as required by the eGovernment Act of 2002, Pub. L. 107–347§208(b)(1)(B)(iii), serves to notify Beneficiaries and Providers calling into the Call Center about the collection and storage of personal information.

Privacy Risk: Privacy Information is used or disclosed outside of its intended purpose.

Mitigation: This PIA serves to notify Veterans calling into the Call Center about the collection and storage of personal information. All callers are informed via the Interactive Voice Recognition (IVR) that each call is being recorded.

Section 7. Access, Redress, and Correction

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

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

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

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

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

For information stored within Salesforce, the following steps are required for making a FOIA request:

- Be in writing (submitted via US Mail, special carrier, fax or email). If the requested records concern your personal privacy or that of another person, then the request must be signed
- Reasonably describe the records so they may be located with a reasonable amount of effort.
- State your willingness to pay applicable fees or provide a justification to support a fee waiver.
- Include a daytime telephone number and/or email address in case we need to contact you.
- Be submitted to the facility that maintains the records.

If the caller doesn't know where the records are located, have them submit their request to:

- By Email: vacofoiaservice@va.gov
- By Mail: FOIA SERVICE 810 Vermont Avenue, NW (005R1C) VACO Washington, DC 20420
- By Fax :202-632-7581

If individuals are requesting access to information from other systems, then they can gain access to their information via those authoritative systems of record.

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 this is not a formal system of record, there are no formal processes for correcting inaccurate information.

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.

The Veteran or their beneficiaries are responsible for maintaining the accuracy of the data so that the Salesforce services can be provided. This information is collected for the purposes of contracting with or providing services to Veterans and is captured in the normal course of conducting business. The Veteran should correct or update the data as necessary during the intake process. Since this system is not a formal system of record, there are no formal processes for correcting inaccurate inform

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

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

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

The system is designed so that the self-service features are optional. Alternatively, Operations Managers and Providers can update information on the Veteran's behalf.

If the individual discovers that incorrect information was provided during intake and is wishing to obtain more information about access, redress, and record correction should contact the Department of Veterans Affairs regional as direct in the National Patient Databases-VA (121VA19) SORN, available at http://www.gpo.gov/fdsys/pkg/FR-2004-04-07/pdf/04-7821.pdf

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Privacy Risk: If individuals are not provided sufficient guidance regarding the access, redress, and correction of their data, then individuals could initiate adverse personnel actions against the Government.

Mitigation: By publishing this PIA, VA makes the public aware of methods for correcting their records. Because this system does not hold authoritative records long-term, it is unlikely individuals will feel the need to correct their information in this system.

Section 8. Technical Access and Security

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

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

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

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

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

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

The VA SF platform is accessible to both internal and external users 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/or AccessVA (SSOe). SFDP VA Assessing entity 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.

Following IAM User Provisioning as implemented for VA Salesforce Community, user role's identity the information and application components a user can access. To receive access to VA Salesforce another system user with appropriate permissions must sponsor them. The sponsor will describe which functionality 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 control of the information and data.

This information is documented in the user provisioning process with the Digital Transformation Center.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, 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 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.

Crystal Moultrie serves as the VA Contract Officer's Representative (COR) for the Salesforce DTC contract and with the VA Salesforce System Owner, Drew Myklegard, maintains 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 VA Salesforce. Michael Domanski will monitor and reviews VA Salesforce related support contracts on a regular basis to ensure no gaps in support for the platform and community users. Developers do not have access to production PII.

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?

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

1. The Security Plan Status: Approved
2. The Security Plan Status Date: 24-Feb-2021
3. The Authorization Status, Authorization to Operate (ATO)
4. The Authorization Date, March 18, 2021
5. The Authorization Termination Date, December 17, 2023
6. The Risk Review Completion Date: 12-Mar-2021
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH). Moderate

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, 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.

This question is related to privacy control UL-1, Information Sharing with Third Parties.

The WHHL is minor application that is hosted on the Salesforce Development Platform VA Assessing and is hosted in a FedRAMP certified cloud. The Salesforce Government Cloud Assessing was granted a full ATO by Deputy CIO Service Delivery and Engineering (SD&E). The IT System name is Salesforce Development Platform (SFDP) VA Assessing, it is owned by the Office of Information Technology (OI&T), Enterprise Program Management Office (ePMO).

Per the approval of the Deputy Assistant Secretary, IT Operations and Services (ITOPS) [the VA Authorizing Official (AO)], Salesforce Development Platform VA Assessing was granted a ATO on March 18, 2021. This ATO will expire on December 17, 2023. The FIPS 199 classification of the system is MODERATE.

9.2 Identify the cloud model being utilized.

Example: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

The Salesforce Development Platform VA Assessing is a commercially available Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) product. The Salesforce Government Cloud Assessing is maintaining the underlying physical infrastructure.

9.3 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)

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

The VA Salesforce Development Platform VA Assessing Cloud Services contract establishes VA ownership rights of all data including PII. The contract information is as follows: Contract Number: VA118-16-D-1008; Task Order Number: 36C10B19N10080030. The contract is set to conclude on June 25, 2024.

9.4 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 Salesforce contract establishes VA ownership rights of all data. The contract stipulates 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.

9.5 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."

9.6 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

The use RPAs or "bots" are not implemented within the WHHL application.

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**

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

Signature of Responsible Officials

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

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2021.11.10 22:47:49 -05'00'

Privacy Officer, Rita Grewal

James C. Boring 149438

Digitally signed by James C. Boring 149438
Date: 2021.11.10 11:52:19 -05'00'

Information Systems Security Officer, James Boring

Michael S. Domanski 326889

Digitally signed by Michael S. Domanski 326889
Date: 2021.11.10 12:04:50 -05'00'

Information System Owner, Michael Domanski

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

Link to the Privacy Policy found here