Privacy Impact Assessment for the VA IT System called:

Salesforce Veterans Crisis Line Chat

Veterans Health Administration

Clinical Services: Office of Mental Health & Suicide Prevention

Date PIA submitted for review:

08/29/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Aaron Cork	Aaron.Cork@va.gov	605-728-4845
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842-2000, Ext: 4613
Information System Owner	Mike Domanski	Michael.Domanski@va.gov	727-595-7291

Abstract

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

The Salesforce Veterans Crisis Line Chat (SF VCL Chat) is a Salesforce module supporting the Veterans Health Administration (VHA) National Mental Health Program. Through its users, the chat module collects data from/about veterans in need and dispatches aid to those veterans that require immediate assistance. The application is hosted on the Salesforce platform and is not public facing. VCL Chat personnel log in to the Salesforce module and create a record based upon the information provided by the chatter. This information may then be accessed by Suicide Prevention Coordinators (SPC) at local VA facilities if the call warrants follow up to resolve the issue. Collected data is not shared with other organizations.

Overview

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

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

The IT system name is Salesforce: Veterans Crisis Line Chat. The Program Office is Clinical Services – Office of Mental Health & Suicide Prevention. The Product Line is Veterans Relationship Management within the Veterans Experiences Service Portfolio.

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.

The chat module allows veterans or individuals concerned about a veteran to communicate with the Veteran Crisis Line responders, who can then dispatch aid to veterans in crisis who require immediate assistance.

C. Indicate the ownership or control of the IT system or project.

The system is VA Controlled and non-VA Owned and Operated.

2. Information Collection and Sharing

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

Approximately 1,000,000 veterans or individuals calling in regarding veterans will be served by the system. The typical affected individual will be a veteran in crisis.

E. A general description of the information in the IT system and the purpose for collecting this information.

Salesforce – Veterans Crisis Line Chat may contain identification, demographic, military history, and medical data provided in a chat by the veteran or the individual calling in regarding a veteran to assist the VCL team with providing support to the veteran, ensuring appropriate follow-up care is provided. In addition, the information will be used for statistical reports for the purpose of evaluating the need for development of further suicide prevention efforts to include education and research. These statistical reports will also be used to provide information related to suicide to VA officials, congressional members, and the public.

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

The SF VCL Chat system will not share data with other systems.

G. *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.*

The system is a cloud-based, enterprise Platform as a Service (PaaS). Therefore, all PII is centrally maintained from a single site. The same use and controls apply to all remote users of this system.

3. Legal Authority and SORN

H. *A citation of the legal authority to operate the IT system.*

Although Salesforce – Veterans Crisis Line Chat data is stored in the Salesforce FedRAMP cloud, it remains the property of the VA and as such, the VA remains responsible for the security and privacy of this data.

The VA enforces these protection requirements through the implementation of its cybersecurity policies and the Risk Management Framework (RMF) process. Under the RMF Process, the system has a Data Security Categorization of High, with the impacts of a data compromise being identified in the Salesforce – Veterans Crisis Line Chat Data Security Categorization (DSC) memo. The Privacy Act of 1974, set forth at 5 U.S.C. 552a, states the legal authority to utilize this information.

System of Records Notice: *Veterans Crisis Line Database SORN 158VA10* 2023-12401.pdf (govinfo.gov).

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

This SORN covers cloud usage and storage. This SORN is not in the process of being modified. *Veterans Crisis Line Database SORN 158VA10* 2023-12401.pdf (govinfo.gov).

D. System Changes

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

Completion of this PIA will not result in changes to business processes.

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

Completion of this PIA will not result in changes to technology.

Section 1. Characterization of the Information

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

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

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

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

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

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

☒ Name

☒ Social Security Number

☒ Date of Birth

☐ Mother's Maiden Name

☒ Personal Mailing Address

☒ Personal Phone Number(s)

☐ Personal Fax Number

☒ Personal Email Address

☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)

☐ Financial Information

☐ Health Insurance Beneficiary Numbers Account numbers

☐ Certificate/License numbers*

☒ Vehicle License Plate Number

☒ Internet Protocol (IP) Address Numbers

☒ Medications

☒ Medical Records

☒ Race/Ethnicity

☐ Tax Identification Number

☐ Medical Record Number

☒ Gender

☐ Integrated Control Number (ICN)

☒Military History/Service Connection

☐ Next of Kin

☒ Other Data Elements (list below)

- VA Employee PIV Electronic Data Interchange Personal Identifier (EDIPI)
- Member of the Public/Individuals Name
- Members of the Public/Individuals Address

- Members of the Public/Individuals Personal Phone

PII Mapping of Components (Servers/Database)

SF VCL Chat consists of 0 (zero) key component (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by SF VCL Chat 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

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
N/A	N/A	N/A	N/A	N/A	N/A

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

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

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

The veteran, family member or anonymous individual may enter information about a veteran into VCL Chat. Veteran Crisis Line Chat Operators may collect information during a chat with the veteran, family member or anonymous individual who initiated the chat.

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

Information from sources other than the individual is not required for this system.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

The system does not create information.

1.3 How is the information collected?

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

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

Information is collected directly from the individual contacting the VCL (the veteran, a friend or family member, or an anonymous caller) over the Veterans Crisis Line Chat text messaging service.

1.3b 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 system does not collect information on a form and is not subject to the Paperwork Reduction Act.

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

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

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

Information provided about a veteran during the chat will be assumed accurate. However, if identifying information about the veteran is voluntarily shared during the chat, the responder may then look up the veteran's medical record to validate information provided in the chat.

1.4b 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 system does not check for accuracy by accessing a commercial aggregator of information.

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 Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that govern the collection, maintenance, use, and dissemination of information about individuals that are maintained in systems of records by federal agencies.

The SORN for the system states the authority of maintenance of the system listed in question 1.1 falls under the following: *Veterans Crisis Line Database SORN 158VA10*
2023-12401.pdf (govinfo.gov)

The SORN 24VA10A7 Patient Medical Records-VA Federal Register :: Privacy Act of 1974; System of Records applies to accessing veterans' medical records if the veterans' identifying information is provided during the chat.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk:
SF-VCL Chat application collects Personally Identifiable Information (PII) and Personal Health Information (PHI) to identify and understand the veteran's situation. If this information were breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.
Mitigation:
SF-VCL Chat uses two-factor authentication to prevent unauthorized access to the system. Additionally, the system can only be accessed by authorized personnel with access to the VA intranet. There is no public access to the system. The Department of Veterans Affairs is careful to only collect the information

necessary to identify the veteran in crisis, identify the potential issues and concerns, and offer assistance to the veteran so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA can better protect the veteran's information. Once collected, information is transmitted using encryption and stored in secure servers behind VA firewalls.

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.

Veteran Identifying Number (can be a unique number or the SSN) – Used as an identifier
Veteran First Name – Used as an identifier
Veteran Last Name – Used as an identifier
Veteran Personal Email – Used to contact individual
Veteran Personal Phone – Used to contact individual
Veteran Address – Used to contact individual
Emergency Contact – Used to contact individual
Veteran License Plate – Used to identify location of the individual
Veteran IP Address – Used to identify location of the individual
Veteran Gender – Used for healthcare support
Veteran Race – Used for healthcare support
Veteran Ethnicity – Used for healthcare support
Veteran Medications – Used for healthcare support
Medical Records – Used for healthcare support
Military History – Used to understand service history

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

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

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

Data gathered and stored in the SF-VCL Chat system is used to help assist Veterans with crisis situations. Statistical reports are created to understand chat trends and help develop the program. These reports do not contain any privacy information that can be connected to a chatter and no new records are created by this process.

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.

New information gathered during chats is added to a record in the SF-VCL Chat. The information gathered during the chat is used to provide the veteran with any care necessary to address their crisis situation. If the veteran agrees to be referred to a Suicide Prevention Coordinator, this information collected during the chat may subsequently be manually added to the veteran’s existing medical record by the Suicide Prevention Coordinator. The information will be accessible to Veterans Affairs employees who make determinations about veteran health care.

2.3 How is the information in the system secured?

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

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

Data in transit are protected by HTTPS site-to-site encryption. PII/PHI data are encrypted at rest with Salesforce Shield encryption.

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

All SSNs are encrypted in all states only visible to VCL internal staff. SSN is PII data, encrypted at rest with Salesforce Shield encryption. Only VA employees with a business need will have the record view based on security levels.

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

SF-VCL Chat is an encrypted, secure system. User roles determine who has visibility into PII/PHI.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. ***Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system***

<u>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.

2.4a How is access to the PII determined?

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

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

Yes, controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA and Salesforce have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the Acting Assistant Secretary for Information Technology [the VA Authorizing Official (AO)]. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how Veterans' information is used, stored, and protected.

2.4c Does access require manager approval?

Yes, managers must approve any new users accessing the system.

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

Yes, VA Identify and Access Management (IAM) systems verify credentials and collect audit logs based on access requested and may contain PII that might have been captured to authenticate to the resource.

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

Accessibility to data is granted based on the permission sets and role-based hierarchy applied based on FedRAMP Salesforce Gov Cloud Plus platform. Account creation is managed and offered through VA via two factor authentication (2FA) Personal Identity Verification (PIV) card and/or Access VA. 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 following data is retained:
Veteran Identifying Number (can be a unique number or the SSN) – Used as an identifier
Veteran First Name – Used as an identifier
Veteran Last Name – Used as an identifier
Veteran Personal Email – Used to contact individual
Veteran Personal Phone – Used to contact individual
Veteran Address – Used to contact individual
Emergency Contact – Used to contact individual
Veteran License Plate – Used to identify location of the individual
Veteran IP Address – Used to identify location of the individual
Veteran Gender – Used for healthcare support
Veteran Race – Used for healthcare support
Veteran Ethnicity – Used for healthcare support
Veteran Medications – Used for healthcare support
Medical Records – Used for healthcare support
Military History – Used to understand service history

3.2 How long is information retained?

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

The information is retained following the policies and schedules of VA's Records Management Service, General Control Schedule 10-1 can be found at the following link: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

The National Department of Veteran Affairs Veterans Crisis Line. This crisis line provides emergency crisis intervention for Veterans throughout the United States. This center operates 24/7/365 in Canandaigua, NY, or any other future location and provides crisis modification via phone, chat, and text: rescue services for high-risk situations; follow-up with caregivers at the local VAMC to verify patient has been contacted and is involved in a plan of care; education and information for callers about local VAMC & community resources; and warm transfers to local support agencies. Call responders at Canandaigua and Suicide Prevention Coordinators (SPCs) at facilities across the country use the VCL software, which is hosted at the Austin Information Technology Center (AITC) in Austin, TX, to log clinical information obtained on the call and share relevant data for Veterans who are referred for additional care in support of the plan of care.
Disposition Instructions: Temporary. Cutoff at end of FY. Destroy when 4 years old.
Disposition Authority: DAA-0015 2017-0001 0001

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

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

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

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

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

SFGCP complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6500. Records contained in the Salesforce FedRAMP cloud will be retained if the information is needed in accordance with a NARA-approved retention period. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). SFGCP records are retained according to the Record Control Schedule 10-1 Section 4 (Disposition of Records). Request for Records Disposition Authority. Disposition Authority: DAA-0015-2013-0004.

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.

All electronic storage media used to store, process, or access records will be disposed of in adherence with the VA Directive 6500. https://www.va.gov/vapubs/search_action.cfm?dType=1

Yes, the system adheres to the VA Directive 6500 and procedures for destruction, elimination or transfer of sensitive personal information. Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. 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. Digital media is shredded or sent out for destruction.
https://www.va.gov/vapubs/search_action.cfm?dType=1

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

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

Patient data is not used in the testing of the application. This is monitored by the application administrators.

For training, SF-VCL Chat either creates test files which do not include actual Veteran data, or if we use Veteran data all such files are reviewed and if applicable, all PHI and PHI is redacted by the privacy officer.

For research, SF-VCL Chat is governed under Office of Mental Health and Suicide Prevention (OMHSP), and anyone using this information for research purposes must follow the Office of Mental Health and Suicide Prevention Data Use Agreement (DUA) Policy. SF-VCL Chat is a subordinate element of OMHSP.

For program evaluation, SF-VCL Chat is governed under Office of Mental Health and Suicide Prevention (OMHSP), and anyone using this information for evaluation purposes must follow the Office of Mental Health and Suicide Prevention Veterans Crisis Line Standard Operating Procedure for Research and Evaluation. SF-VCL Chat is a subordinate element of OMHSP.

Users accessing the system must undergo basic Privacy training such as, Privacy and Information Security Awareness and Rules of Behavior and information security training annually.

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 ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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.

Follow the format below:

Privacy Risk: There is a risk the information maintained by SF VCL Chat could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk posed by information retention, the SF VCL Chat module adheres to the VA Records Control Schedules for each category or data it maintains. When the retention data is reached for a record, SF VCL Chat disposes of the data by the determined method as described in question 3.4. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)", contains the policies and responsibilities that VA components are required to follow to manage data breaches, including detection, correlation, notification, remediation, and reporting.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
IAM (Identity Access Management)	Single Sign on Authentication System - authenticates a SF VCL Chat personnel is an authorized user	Name, SecID, DUZ (Designated User ID), Access Token	Electronic Transfer using Secure Socket Layer (SSL) Encryption
Microsoft Active Directory Federated Services (ADFS)	Contingent Single Sign on Authentication System – validates that SF VCL Chat personnel are authorized users	Name, SecID, Work Email Address	Electronic Transfer using Secure Socket Layer (SSL) Encryption

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: There is a risk that information may be shared with an unauthorized VA program or system or that data could be shared.

Mitigation: The principle of need-to-know is strictly adhered to by the SF VCL Chat personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system. Safeguards implemented to ensure data is not sent to the wrong VA organization include employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV)/USAccess Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all security measures that are utilized.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

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

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

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

Follow the format below:

<u>Privacy Risk:</u> Not applicable.

<u>Mitigation:</u> Not applicable.

Section 6. Notice

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

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

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

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

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in two ways:

1. The Veterans Crisis Line Database SORN 158VA10NC5 defines the information collected from Veterans, use of the information, and how the information is accessed and stored.
2. This Privacy Impact Assessment (PIA) also serves as a notice of this system.

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

Notice was provided via the SORN and this PIA.

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

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in two ways:

1. The Veterans Crisis Line Database SORN 158VA10NC5 defines the information collected from Veterans, use of the information, and how the information is accessed and stored.
https://department.va.gov/privacy/system-of-records-notices/

2. This Privacy Impact Assessment (PIA) is posted on the internet and also serves as a notice of this system. Veterans Crisis Line Database SORN 158VA10NC5

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.

Veterans who send a chat to the Veterans Crisis Line Chat are asked questions and they can decline to answer any question, though a denial to provide information may result in the chat employee not having all the information needed to make referrals. No penalty will occur, and veteran benefits will not be affected or denied.

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.

Veterans who send a chat to the Veterans Crisis Line Chat voluntarily provide information and are notified that the information they provide will only be used to assist in helping the Veteran through their crisis. Other than refusing to participate, individuals do not have a right to consent to particular uses of the information or to review or to contest the information in this system because the system is only used to assist the Veteran through their crisis.

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 System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

Follow the format below:

Privacy Risk: There is a risk the individual does not understand that data from a text to the SF VCL Chat has been captured in a database. Risk is associated with individuals being unaware the SF VCL Chat system exists within the Department of Veterans Affairs.

Mitigation: The Veteran is notified that the information is entered in a database by the publication of SORN# 158VA10NC5, Veterans Crisis Line Database-VA. Also, this Privacy Impact Assessment (PIA) is posted on the internet and serves as a notice of this system. The VA mitigates this risk of individuals being unaware the system exists by providing the public with notice that the system exists, as discussed in detail in question 6.1.

Section 7. Access, Redress, and Correction

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

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

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

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

As per the *Veterans Crisis Line Database SORN 158VA10* 2023-12401.pdf (govinfo.gov), Individuals seeking information on the existence and content of records in this system pertaining to them should contact vhavclprivacy@va.gov or call the Veterans Crisis Line for assistance. A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.
SYSTEM MANAGER(S): Official responsible for policies, procedures, and system of records; Acting Executive Director, Office of Mental Health and Suicide Prevention, 810 Vermont Avenue NW, Washington, DC 20420; (513) 233–1748 (this is not a toll-free number).

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).

This 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.

This system is a Privacy Act system.

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 seeking to contest or amend records in this system pertaining to them should contact VHAVCLRequestsforInformation@va.gov or call the Veterans Crisis Line for assistance. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

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.

Generalized notice is provided by the publication of the Veterans Crisis Line SORN 2023-12401.pdf (govinfo.gov).

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Formal redress is provided through the Privacy Act and Freed of Information Act (FOIA).

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 System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

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

Follow the format below:

Privacy Risk: There is a risk the Veteran does not know what information has been retained after sending a text to the VCL Chat. The propensity exists for incorrect information provided, captured, or entered during a call to remain that way. Risk is associated with individuals having no proper guidance regarding access, redress and correction of their information being captured by the SF VCL Chat system.

Mitigation: Individuals who wish to determine whether this system of records contains information about them should contact vhavclprivacy@va.gov. Inquiries should include the person's full name, phone number, date of birth, and email or mailing address. An end user can reach out to VHA VCL Requests by contacting vhavclprivacy@va.gov or call the Veterans Crisis Line (Dial 988 and then press 1) for the correct process to address data inaccuracies. By publishing this PIA and the applicable SORN, the VA makes the public aware of the information being captured by the SF VCL Chat 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?

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.

System access to the Veterans Crisis Line is restricted to System Administrators, chat personnel, and Suicide Prevention Coordinators (SPC) at local VA facilities.
a) System Administrators have elevated privileges on the system and are granted access by following the Enterprise Operations (EO) 9957 process which is a method used by the VA to ensure that only those who require access are granted access.
b) SF VCL Chat personnel enter information into the Veterans Crisis Line application web interface, documenting the caller information and the perceived crisis. These users have read/write access via the web interface. Personnel receive access through a written request to their Chat administrative officer who approves the request and forwards it to Clinical Application Coordinator (CAC). The CAC then creates the account with the appropriate permissions.
c) Suicide Prevention Coordinators (SPC) at local VA facilities can access the information entered into VCL by personnel to review the information before contacting the caller for local support. SPC receive access through a written request from their supervisor to the Clinical Application Coordinator. The CAC then creates the account with the appropriate permissions.

Per VA Directive 6500, the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

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 government agencies do not have access to the system..

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.

Role-based hierarchy of profiles and permission sets are applied for users accessing the platform. Only authorized VA users can access this tool. Users access the SF VCL Chat system using Single Sign On (SSO) and two factor authentication to log in. Additionally, field audit trails and event monitoring provided by Salesforce platform assists in ensuring only assigned users have access to specific records within the Salesforce.

a) System Administrators have elevated privileges on the system and are granted access by following the Enterprise Operations (EO) 9957 process which is a method used by the VA to ensure that only those who require access are granted access.

b) Personnel enter information into the SF VCL Chat, documenting the chat information and the perceived crisis. These users have read/write access to SF VCL Chat. Personnel receive access to SF VCL Chat through a written request to their Chat administrative officer who approves the request and forwards it to Clinical Application Coordinator (CAC). The CAC then creates the account with the appropriate permissions.

c) Suicide Prevention Coordinators (SPC) at local VA facilities can access the information entered into SF VCL Chat by personnel in order to review the information before contacting the caller for local support. SPC receive access through a written request from their supervisor to the Clinical Application Coordinator. The CAC then creates the account with the appropriate permissions.

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, have access to the VA Salesforce system and the PII and VA Sensitive Information data contained therein, and supports the SF VCL Chat application when an outage occurs. 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 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 of SF VCL Chat. The ISO will monitor and review VA Salesforce related support contracts on a regular basis to ensure no gaps in support for the users.

The contracted system integrators or developers working on the system utilize dummy/test data while configuring and testing the system. Developers do not have access to production PII. Contractors are required to sign a Business Associate Agreement (BAA).

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.

General Training includes VA Privacy and Information Security Awareness and Rules of Behavior, TMS 10203 - Privacy and Health Insurance Portability and Accountability Act (HIPPA), VA On-boarding enterprise-wide training, and annual information security training. After the user's initial acceptance of the Rules, the user must reaffirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the Talent Management (TMS) system.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 04/05/2023
3. *The Authorization Status:* Active
4. *The Authorization Date:* 08/07/2023
5. *The Authorization Termination Date:* 08/06/2025
6. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Not applicable.

Section 9 – Technology Usage

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

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

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

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

Yes, the SF VCL Chat system utilizes Salesforce Gov Cloud Plus. Salesforce Government Cloud Plus is hosted in the AWS GovCloud. The Salesforce Government Cloud Plus (SFGCP-E) is built on the underlying Salesforce Force.com that is hosted in a FedRAMP Certified FISMA High environment which is in the Amazon Web Services (AWS) GovCloud West. This software utilizes the PaaS Service of Salesforce Gov Cloud Plus. The SF VCL Chat module is housed in Government Cloud on the FedRAMP-authorized Salesforce Government Cloud Plus (SFGCP), eMASS IDs 1295 & 1296.

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

Yes, VA has full ownership of the PII/PHI that will be shared through SF VCL Chat. Contract agreement "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B.

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.

Ancillary data is not collected by Salesforce. VA has full ownership over the data stored in the SF VCL Chat system.

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.

VA has full authority over the data stored in the SF VCL Chat system.

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 utilize 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 provided in this Privacy Impact Assessment is true and accurate.

Aaron L. Cork

Digitally signed by AARON CORK
Date: 2023.09.07 10:40:26 -05'00'

Privacy Officer, Aaron Cork

JAMES
BORING

Digitally signed by JAMES
BORING
Date: 2023.09.08 08:55:02
-04'00'

Information Systems Security Officer, James Boring

MICHAEL
DOMANSKI

Digitally signed by MICHAEL
DOMANSKI
Date: 2023.09.08 08:51:35 -04'00'

Information Systems Owner, Mike 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).

SORN# 158VA10NC5, Veterans Crisis Line Database-VA

SORN# 24VA10A7 Patient Medical Records-VA

VA System of Records Notices: https://department.va.gov/privacy/system-of-records-notices/

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

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices