Privacy Impact Assessment for the VA IT System called:

Veterans Crisis Line

ENTERPRISE PROGRAM MANAGEMENT OFFICE (EPMO)

Date PIA submitted for review:

1/6/2022

System Contacts:

	Name	E-mail	Phone Number
Privacy Officer	Aaron Cork	Aaron.Cork@va.gov	(605) 728-4845
Information System Security Officer (ISSO)	Anthony Robinson	Anthony.Robinson@va.gov	(785) 350-1822
Information System Owner	Delwin Johnson	Delwin.Johnson2@va.gov	(202) 367-4033

Abstract

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

The Veterans Crisis Line (VCL) application is a web-based system which collects data from veterans in need of suicide prevention assistance and dispatches aid to those veterans that require immediate assistance. The application is hosted at the Austin Information Technology Center (AITC).

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?*

In 2007, Congress passed the *Joshua Omvig Veterans Suicide Prevention Act of 2007,* Pub. L. 110-110, 121 Stat. 1031 to create a comprehensive program for suicide prevention among veterans. In response to this act, the Department of Veterans Affairs launched the Veterans Crisis Line (VCL) (formerly National Veterans Suicide Prevention Hotline) that same year. Since its inception, the VCL has answered more than 1.1 million calls and made more than

37,000 lifesaving rescues. The application sends data provided by the caller to VistA. It does not acquire medical data ***from*** VistA

In 2009, the VCL added an anonymous online chat service, and in November 2011, the VCL introduced a text messaging service to provide another way for Veterans to connect with confidential, round-the- clock support. To support the important work of this program, the Department of Veterans Affairs (VA) has created the Veterans Crisis Line (VCL) system. It is a web-based Veterans Health Administration (VHA), National Mental Health Program, owned major application which collects data from veterans in need of suicide prevention and dispatches aid to those veterans that require immediate assistance. The application is hosted at the Austin Information Technology Center (AITC).

When a veteran and/or their families and friends become concerned about a veteran in potential emotional crisis, they may contact the Veterans Crisis Line via confidential toll-free hotline, online chat, or text. Through these mediums, they are connected with qualified, caring Department of Veterans Affairs responders who staff the VCL call center. When a VCL responder is contacted by a veteran or concerned friends or family, the responder will speak with the individual about the potential crisis. Information gathered through phone conversations or text messages are used to create a record for the Veteran in the VCL application. Information obtained through chat is not recorded. Every VCL recording contains the same basic contents: date of initial call/text message received, name of potentially affected veteran, phone number of the veteran, and description of the concern. The record is stored in the VCL application and is synchronized with Veterans Health Information Systems and Technology Architecture (VistA), Compensation, Pension Records Interchange (CAPRI), and Suicide Data Repository (SDR) using the provided social security number. If the Veteran agrees to further consultation, the information will then be accessed by Suicide Prevention Coordinators (SPC) at a local VA support facility. The need for follow up activity is determined at the time of the call.

The Veterans Crisis Line and its associated applications operate under the authority of *Joshua Omvig Veterans Suicide Prevention Act of 2007,* Pub. L. 110-110, 121 Stat. 1031 which gives the VA Secretary the authority to develop and carry out a comprehensive program designed to reduce the incidence of suicide among veterans. This act amended Title 38 of the United States Code by including *Comprehensive program for suicide prevention among veterans,* Title 38 U.S.C. § 1720F as part of the law.

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 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
- ☒ Gender
- ☐ Integration Control Number (ICN)
- ☒ Military History/Service Connection
- ☐ Next of Kin
- ☐ Other Unique Identifying Information (list below)

Only information pertinent to the call and known to the caller is collected. The information collected is used to understand and help resolve the veteran's crisis. The Veterans Crisis Line attempts to aid Veterans with any situation that may be perceived by the Veteran as a crisis and information collected varies depending upon the situation.

PII Mapping of Components

Veterans Crisis Line consists of one key component. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Veterans Crisis Line and the reasons that collect it are mapped 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. The first table of 3.9 in the PTA should be used to answer this question.

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
Suicide Data Repository	Yes	Yes	Name, SSN, DOB, Address, Email, License Plate, Race/Ethnicity, Medication, Medical Records, Gender, Military History/Service Connection	Used to identify the veteran	Encryption in all states

PII is collected from the caller and stored by the Hotline database. When necessary or appropriate the data is forwarded to CPRS for action by a Suicide Prevention Councilor.

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.

Crisis Hotline Call Center Operators collect information from callers, transcribe from the medical record, and input that data manually into the Veterans Crisis Line (VCL) web application.

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 is transcribed from the veteran's medical record and collected directly from the individual contacting the VCL (whether the veteran themselves, or a concerned friend or family member) over the Veterans Crisis Line telephone and text messaging services.

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.

Some information is validated against the medical record and information received from the caller is not checked for accuracy. It is assumed callers are providing accurate 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 Veterans Crisis Line and its associated applications operate under the authority of *Joshua Omvig Veterans Suicide Prevention Act of 2007,* Pub. L. 110-110, 121 Stat. 1031 which gives the VA Secretary the authority to develop and carry out a comprehensive program designed to reduce the incidence of suicide among veterans. This act amended Title 38 of the United States Code by including *Comprehensive program for suicide prevention among veterans,* Title 38 U.S.C. § 1720F as part of the law.

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.

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, collects 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:

The Veterans Crisis Line (VCL) application collects Personally Identifiable Information (PII) and information regarding 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:

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.

Name: Used to identify the veteran who is in need of help, the call responder and Suicide Prevention Coordinator (SPC)
Social Security Number: Used to verify the identity of the veteran before synchronizing the VCL record with VistA
Date of Birth: Used to verify the identity of the veteran
Mailing Address: Used to verify the identity of the veteran
Phone Number(s): Used to contact the veteran
Email: Used to contact the veteran
Emergency Contact Information: Used to identify emergency contact of veteran
Vehicle License Plate: Used to verify identity of the veteran
Internet Protocol (IP) Address Numbers: Used to identify the location of the veteran
Current Medications: Used to identify current medications of the veteran
Previous Medical Records: Used to identify previous medical records of the veteran
Race/Ethnicity: Used to identify the identity of the veteran
Gender: Used to identify gender of the veteran
Military History/Service Connection: Used to identify service history of the veteran

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

Data gathered and stored in the Veterans Crisis Line system is used to help assist Veterans with crisis situations. Statistical reports are created to understand call trends and help develop the program. These reports do not contain any privacy information which can be connected to a caller and no new records are created by this process.

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?

Encryption 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?

SSNs are masked on records marked "Sensitive" while in VistA, during the lookup and prior to pulling the data into the call record. All SSNs are entered into a secure database, encrypted in all states only visible to VCL internal staff.

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

Encryption in all states.

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

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. 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. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

*Principle of Transparency: Are t*he PIA and SORN clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Data gathered and stored in the Veterans Crisis Line system is used to help assist veterans with crisis situations. All personnel with access to the Veterans Crisis Line information system receive annual privacy training, and are required to sign a document outlining what behaviors are allowed and not allowed on a US Government computer system.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is retained by the system.
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

Name, Social Security Number, Date of Birth, Mailing Address, Phone Number(s), Email Address, Emergency Contact Information, Vehicle License Plate Number, Internet Protocol (IP) Address Numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Gender, Military History/Service Connection.

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.

VCL is presently maintaining these electronic records as Unscheduled-Permanent records, pending submission of new schedule proposal to NARA, due to changes in operational and clinical needs since the previous record schedule was published.

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.

The VCL is currently covered by the NARA Record Schedule DAA-0015-2017-001with a 4-year retention period. This retention period has been deemed to be too short to support ongoing clinical, operational, and research needs. While call recordings and paper records will continue to be destroyed according to this 4-year retention schedule, all other electronic records will be maintained as unscheduled permanent records until a new record schedule is established with NARA.

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

Paper records are transferred to National Archive and Record Administration federal record centers and are securely destroyed once they have reached their disposition age. Call recordings are securely deleted after they have reached their 4-year retention period. All other electronic records are maintained as unscheduled permanent records, pending the approval of a new record retention schedule.

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

Patient data is not used in the testing of the application. This is monitored by the application administrators. For training, VCL either creates test files which does 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, VCL is governed under Office of Mental Health and Suicide Prevention (OMHSP) data use, see attached policy governing this area. VCL is a subordinate element of OMHSP.

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.

Follow the format below:

Privacy Risk:

There is a risk the information maintained by VCL 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 VCL system adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, VCL 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***
Suicide Data Repository (SDR)	Data shared to update records in SDR	Name, SSN, DOB, Address, Email, License Plate, Race/Ethnicity, Medication, Medical Records, Gender, Military History/Service Connection	Electronic Transfer using Secure Socket Layer (SSL) encryption
Veterans Health Information Systems and Technology Architecture (VistA)	Veteran information is validated	Name and SSN are received from VistA into Medora	Electronic Transfer using Secure Socket Layer (SSL) encryption
Compensation, Pension Records Interchange (CAPRI)	Veteran information is validated	No PII is exchanged	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.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk:

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

Mitigation:

The principle of need-to-know is strictly adhered to by the Veterans Crisis Line 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 measures that are utilized within the facilities.

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

VCL does not share data with organizations external to the VA.

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				

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

Follow the format below:
Privacy Risk: N/A
Mitigation: N/A

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.

Veterans Crisis Line Database SORN 158VA10NC5

The Veteran is notified verbally at the time of the call that the information is being entered into the VCL system. No script is used.

Individuals who wish to determine whether this system of records contains information about them should contact the Office of Mental Health Operations (10NC5). Inquiries should include the person's full name, social security number, dates of employment, date(s) of contact, and return address.

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 call into the Veterans Crisis Line are asked questions and they can decline to answer any question, though a denial to provide information may result in the call center employee not having all the information needed to make referrals.

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 call into the Veterans Crisis Line voluntarily provide information and are notified that the information they provide will only be used to assist in helping 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.

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 call or text to the VCL has been captured in a database.

Mitigation:

The Veteran is notified verbally at the time of the call that the information is being entered into the VCL system. No script is used.

SORN# 158VA10NC5, Veterans Crisis Line Database-VA, provides the categories of records, routine uses, policies and practices, retention and disposal, and the notification procedures. This can be viewed in the Federal Register Vol. 80, No. 79/Friday, April 24, 2015/Notices at https://www.govinfo.gov/content/pkg/FR-2015-04-24/pdf/FR-2015-04-24.pdf

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.

Individuals seeking information regarding access to and contesting of records in this system may write, call, or visit the Office of Mental Health Operations (10NC5).

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.

The information provided by the Veteran is considered to be accurate. The information is gathered to assist with the specific crisis. Inaccurate information can be corrected once the Veteran is under the care of a local facility, but the information stored in the VCL database is not changed and has no impact on the care or services they receive.

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 information provided by the Veteran is considered to be accurate. The information is gathered to assist with the specific crisis. Inaccurate information can be corrected once the Veteran is under the care of a local facility, but the information stored in the VCL database is not changed and has no impact on the care or services they receive.

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 information provided by the Veteran is considered to be accurate. The information is gathered to assist with the specific crisis. Inaccurate information can be corrected once the Veteran is under the care of a local facility, but the information stored in the VCL database is not changed and has no impact on the care or services they receive.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk:
There is a risk the Veteran does not know what information has been retained after calling the VCL.

Mitigation:

Individuals who wish to determine whether this system of records contains information about them should contact the Office of Mental Health Operations (10NC5). Inquiries should include the person's full name, social security number, dates of employment, date(s) of contact, and return address.

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.

System access to the Veterans Crisis Line is restricted to System Administrators, call center 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) Call Center 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. Call Center personnel receive access through a written request to their call center 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 the Call Center 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.

All personnel with access to the Veterans Crisis Line are VA employees.

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.

VA requires TMS (Talent Management System) course 10176 "Privacy and Information Security Awareness and Rules of Behavior" to be completed by all employees and contractors upon initial hiring and annually thereafter.

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 - 12/20/21*

3. *The Authorization Status - Approved*
4. *The Authorization Date - 2/22/17*
5. *The Authorization Termination Date - 2/8/22*
6. *The Risk Review Completion Date - 12/10/21*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH) - HIGH*

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).

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.

The VCL system does not use cloud technology.

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)

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

The VCL system does not use cloud technology.

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

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

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

The VCL system does not use cloud technology.

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

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

The VCL system does not use cloud technology.

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).

The VCL system does not use Robotics Process Automation.

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 Privacy Officers

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

Aaron L. Cork

Digitally signed by AARON L CORK
358417
Date: 2022.01.12 11:50:15 -06'00'

Privacy Officer, Aaron Cork

ANTHONY ROBINSON

Digitally signed by ANTHONY ROBINSON
Date: 2022.01.11 13:08:17 -06'00'

Information System Security Officer, Anthony Robinson

Delwin C. Johnson
110488

Digitally signed by Delwin C. Johnson
110488
Date: 2022.01.12 13:47:50 -05'00'

Information System Owner, Delwin Johnson

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).

Veterans Crisis Line Database SORN 158VA10NC5

Federal Register Vol. 80, No. 79/Friday, April 24, 2015
https://www.govinfo.gov/content/pkg/FR-2015-04-24/pdf/FR-2015-04-24.pdf