Privacy Impact Assessment for the VA IT System called:

Salesforce Veterans Affairs Health Connect Customer Relationship Management

(VAHC CRM)

Office of Veterans Access to Care (OVAC)

Veteran Health Administration

Date PIA submitted for review:

8/23/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	phillip.cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	267-283-7653
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	304-283-7554

Abstract

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

Through the Veterans Affairs Health Connect Customer Relationship Management (VAHC CRM) tool, the Department of Veterans Affairs (VA) is modernizing its Clinical Contact Centers (CCC) to serve as a "virtual front door" to VA health care, providing Veterans additional choices for meeting clinical, pharmacy, scheduling, and administrative needs. Clinical Contact Centers will provide Veterans and their caregivers 24/7, on-demand access to clinical and administrative services to address urgent and episodic health care needs over phone and email.

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?*

The Veterans Affairs Health Connect Customer Relationship Management (VAHC CRM) tool, sponsored by the Office of Veterans Access to Care (OVAC), will modernize the VA's Clinical Contact Centers (CCCs) to provide Veterans additional choices for meeting clinical, pharmacy, scheduling, and administrative needs. By providing basic PII to validate the Veterans identity, CCCs, formally called VA Health Connect, provide Veterans and their caregivers immediate, 24/7, on demand access to clinical and administrative services to address health care needs over the phone, and email. The application is designed to support over eight million Veterans and their caregivers across all Veteran Integrated Service Networks (VISNs), beginning with VISN8 before expanding enterprise wide. VAHC CRM is authorized to operate per legal authority, public law 113-146, Veterans Access, Choice, and Accountability Act of 2014.

The VAHC CRM application is a module based in the VA-authorized Salesforce Software as a Service (SaaS) capability and pulling information from a variety of data sources, including, but not limited to VA Master Person Index (MPI), the VA's Health Data Repository (HDR) and PCCM. Our application delivers four core virtual care services–Scheduling and Administration, Clinical Triage, Virtual Clinic Visits, and Pharmacy –24 hours a day, 7 days a week across VA through a standardized and centralized model.

The following diagram shows the other systems (TXCC Triage, VAEC, VA Data Centers, DTC Integration Platform, ESR, HDR, VA Profile, VDIF, PCMM, MPI, VA Knowledge Base, and Finesse Telephony Servers) with whom VAHC CRM (in the Salesforce Health Cloud) shares data. Since this system is based in the Salesforce cloud, there is only one instance of its data, but it can be reached by all VAHC CRM user across the department. As previously stated, VAHC CRM is a module in the Salesforce SaaS offering and falls under its VA and FedRAMP Authorizations to Operate (ATO).

The primary VAHC CRM goal is to consolidate existing business practices under one umbrella, allowing Veterans to easily reach four core virtual care services. It will not

- Cause any business processes to change,
- Cause any technology changes, nor
- Affect the relevant SORN (SORN for this system is:
- (https://www.oprm.va.gov/privacy/systems_of_records.aspx), SORN 24VA10A7 Patient Medical Records–VA:.
- https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020- 21426.pdf
- AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Sections 501(b) and 304.
- SORN 79VA10 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA: https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf
- AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, section 7301(a).
- SORN 168VA005 Health Information Exchange-VA *https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021- 01516.pdf*
- AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Section 501.

Although VAHC CRM 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. VAHC CRM has a VA ATO. 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 Categorization of High, with the impacts of a data compromise being identified in the VAHC CRM Data Security Categorization (DSC) memo.

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)

PII Mapping of Components

VAHC CRM consists of one (1) key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected VAHC CRM and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VAHC CRM Salesforce.com Database	Yes	Yes	SSN, DOB, Name, Gender, Phone, Fax, Mailing Address, Residential Address, Email Address, Mother's Maiden Name, Next of Kin, Emergency Contact	Identification of individuals; clinical healthcare operations; healthcare administrative functions such as ensuring data VA has on file is kept up to date.	Data in transit is encrypted via Transmission Layer Security (TLS) 1.2. Data is also encrypted at rest.

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.

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.

VAHC CRM ingests data from the table in question 1.2 via electronic transmission. Information is also collected directly from Veterans and their caregivers via phone and video communication modes.

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.

All person records will have an existing MPI Correlation. If a user attempts to create a new record in the CRM, a systematic check is performed against MPI to ensure the correct identity is retried in real-time. A “unique” constraint exists on the Salesforce identity record to ensure that no duplicate VA Identities can co-exists within VAHC CRM.

Data updates of existing information such as Address updates are validated against a VA Profile validation API prior to be written.

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

Per SORN 168VA005 – Virtual Lifetime Electronic Record (VLER)-VA, the authority for maintenance of the system is Title 38, United States Code, Section 501.
https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf

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, 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: VAHC CRM stores sensitive Veterans' PII and PHI The risk is in revealing this information to an unauthorized party.

<u>Mitigation:</u> VAHC CRM uses two-factor PIV-based 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.

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 as an identifier
DOB: Used as an identifier
Sex/Gender: Used for healthcare support
SSN: Used as an identifier
Mother's Maiden Name: Used as an identifier
Blood Pressure: Used for healthcare support
Medication: Used for healthcare support
Labs: Used for healthcare support
Phone Numbers: Used to contact individual
Mailing Address: Used to contact individual
Fax: Used to contact individual
Email: Used to contact individual
Emergency Contact: Used for healthcare administration
Health Insurance Beneficiary Numbers: Used for healthcare administration
Previous Medical Records: Used for healthcare support
Race/Ethnicity: Used for healthcare support
Medical Record number: Used as an identifier
Integration Control Number: Used as an identifier
Military History/Service Connect: Used for healthcare administration
Next of Kin: Used for healthcare administration

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

VAHC CRM will update an existing Veteran's record based on the information provided during the call. This information can be made available to requestors by following the VA's standard procedures for requesting such access. No analysis is performed on the information collected during the triage 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?

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

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

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

All traffic to and from VAHC CRM is encrypted in transit via TLS 1.2 or higher.
All data is encrypted at rest at a database-level due to its residence on Salesforce Government Cloud Plus (FedRAMP High). Further, sensitive PII such as Social Security Numbers are also encrypted at rest (at second time) at the platform level.

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

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

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

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

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

Add answer here:

VAHC CRM follows the standard need-to-know principle of only granting access to VA employees to the data they need to perform their jobs. As part of standard VA Privacy and Information Security training, users are taught not to arbitrarily share data with co-workers unless the co-worker has a need for that data. Anyone needing access to data goes through the formal VA access request process, submitting a SNOW (ServiceNow) ticket and receiving their supervisor's approval before access can be granted. As with all access to PII and PHI, data access is audited to identify possible misuse. Logs of record views are sent to VA Splunk for use by the privacy office.

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

VAHC CRM retains all of the data listed in Question 1.1, specifically, Name, Address, Telecom, Business/VA email address, Role, Primary Location, Locations, Organization, Organization Alias, Organization Address, Organization Telecom, Person and Contact Demographic, Person and Demographic Alias, Person and Demographic Address, Person and Demographic Telecom, Person and Demographic Email, Health Care Provider, Account, Contact Relation, Account Relation, Contact Preferences, Person Identifiers, and Source Person Identifiers.

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.

VAHC CRM is built on Salesforce.com, a Cloud technology. Data sent to VistA from VAHC CRM is considered part of the patient longitudinal record, however health information stored within VAHC CRM is not considered part of a Veteran patient's medical record. Because of this, data generated within VAHC CRM by end users must be archived (removed from VAHC CRM) within four years.

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.

VAHC CRM will follow the NARA Records Schedule DAA-0015-2017-0001 that was established for Department of Veterans Affairs Veterans Health Administration Call Centers.

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

VAHC CRM follows the standard VA policy in disposal of digital data, following the guidelines identified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-81, Revision 1. Since these procedures change with the storage technology and medium being used, VAHC CRM personnel consult SP 800-81R1 and additional OIS guidance prior to disposing of digital data.

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

VAHC CRM does not use PII for research, testing and training.

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.

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: VAHC CRM stores sensitive Veteran PII and PHI. With this quantity of data, there is a risk that unauthorized personnel will attempt to access the data without permission.

Mitigation: To assist in preventing unauthorized access to PII/PHI, VAHC CRM uses two-factor authentication to prevent unauthorized access to the system and accounts are only created for employees who are working VAHC CRM and have a supervisor-validated Need-to-Know (NTK). Additionally, the system can only be accessed by authorized personnel from within the VA intranet, preventing access attempts from outside the intranet.

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***
VA Identity Access Management	Internal VA Employee VistA designated user number and corresponding VistA instance required for writing clinical progress notes and encounters back to VistA.	Internal VA Employee VistA designated user number (DUZ) and corresponding three-digit VistA instance.	Site to Site Encrypted with TLS 1.2
VA Cisco Finesse	Telephony screen pop and click-to-call; reporting performance metrics.	Phone number.	Site to Site Encrypted with TLS 1.2
VA Master Person Index (MPI)	Authoritative system for VA Person Information.	First name, middle, last name, name prefix, name suffix, date of birth, state of birth, country of birth, address, phone, date of death, current gender, mother's maiden name, and SSN.	Site to Site Encrypted with TLS 1.2
VA Primary Care Management Module (PCMM)	Displays the VA and non-VA providers that comprise the care team of a given Veteran patient.	Full names, job titles, phone, pager, fax of the PACT team members.	Site to Site Encrypted with TLS 1.2
VA Profile	Authoritative system for contact information such as phone, address, email, and fax.	Mailing address, residential address, fax, phone (work, mobile, home, temporary), and email.	Site to Site Encrypted with TLS 1.2
VA Health Data Repository (HDR)	Displays clinical information from VistAs.	Clinical data for Consults, Flags, Medications, Progress Notes, Orders, Problems List, Radiology	Site to Site Encrypted with TLS 1.2

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*
		Exams, Visits, Vitals, Discharge Summaries, Immunizations, and allergies/adverse reactions.	
VA Eligibility & Enrollment System (ESR)	Displays registration, insurance, and service- connected information.	Service branches, eligibilities, disability percentage, insurance, health benefit plans.	Site to Site Encrypted with TLS 1.2
VA Corporate Data Warehouse (CDW)	Provides person demographic information.	Full name, SSN, ICN, Phone, and Primary Address.	Site to Site Encrypted with TLS 1.2
Digital Veterans Platform (DVP)	Address validation service.	Address (mailing and residential).	Site to Site Encrypted with TLS 1.2

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 potential loss of information due to theft or destruction with the shared information.

Mitigation: Every internal system with which VAHC CRM shares data has an Authorization to Operate (ATO) that describes how PII and PHI are to be protected. Through Continuous Monitoring, data is protected in accordance with (IAW) the security and privacy controls outlined in their System Security Plans (SSPs) and VA policies and procedures.

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***	***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***	***List the method of transmission and the measures in place to secure data***

	specified program office or IT system		***external sharing (can be more than one)***	

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: VAHC CRM exchanges information with external systems in real time. The risk is in revealing this information to an unauthorized party.

Mitigation: VAHC CRM 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. Data in transit is protected by Transport Layer Security (TLS) version 1.2 or FIPS 140-2 encrypted Virtual Private Network (VPN) tunnels.

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.

Yes**.** VA Form 10-10EZ (Appendix A) and the system's SORN168VA005 https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf are provided as notice's for VAHC CRM. Privacy Act statements are part of all VHA Notice of Privacy Practices which are sent out every 3 years. IB 10-163 Notice of Privacy Practices, https://www.va.gov/files/2022- 02/Notice_of_Privacy_Practices_IB_10-163.pdf, which may be used to submit requests for help.

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

No.

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

No.

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: Patients do not understand to what extent their PII and/or PHI are being collected and how it may be used.

Mitigation: Veterans are informed that their PII/PHI is being collected per their enrollment for health benefits (VA Form 10-10EZ).Privacy Act statements are part of all VHA Notice of Privacy Practices which are sent out every 3 years. IB 10-163 Notice of Privacy Practices: https://www.va.gov/files/2022- 02/Notice_of_Privacy_Practices_IB_10-163.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.

In accordance with VA Directive 6300 and Handbooks 6300.3, Procedures for Implementing the FOIA, 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act, and VHA Directive 1605.1, Privacy and Release of Information an individual's submitting information requests may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned system of records, Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted. Access to Care provider information is publicly available.

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.

Veterans and/or their caregivers wanting to access information in their records can download them via My HealtheVet or by visiting their local VA facility. There are no VAHC CRM specific procedures or regulations on requesting access to one's records.

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.

By contacting the appropriate VHA office. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to, and reviewed by the System Manager for the concerned system of records, Privacy Officer, or their designee.

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.

If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures and process as before with the VA Partner system (VHA), and state that the documentation they are now providing supersedes that previously provided.

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?

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

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

Follow the format below:
<u>Privacy Risk:</u> There is a risk that the Veteran/caregiver-provided information in VAHC CRM is inaccurate and decisions are made with incorrect information and that the Veteran/caregiver could be unaware of access, redress, and correction procedures

<u>Mitigation:</u> VAHC CRM follows VA processes which allow an individual, adequate notification of the data being collected and the limitations of use for the data. A formal VA procedure (listed in 7.1) exists where individuals who wish to determine whether this system of records contains information about them should contact the VA facility location at which they are or were employed or made contact. 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.

General users follow the standard VA account request and creation process by submitting a SNOW ticket and securing the appropriate approvals from supervisors. Users are allowed to create and modify information provided by Veterans and/or their caregivers.

A second type of user is a privileged user who maintains VAHC CRM and complete the required privileged user training, request a privileged account via a SNOW ticket, secure management approval of their account request, and received ePAS access.

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.

Yes, the Contracting Officer Representative (COR) reviews the contract on at least an annual basis. There are contractor system administration personnel who maintain the Salesforce infrastructure but are not users of the VAHC CRM system itself. Liberty IT Solutions employees and sub-contractors who have developed VAHC CRM do not have Production access. All contractors sign a NDA for their employment by the vendor and a HIPPA BAA is in place 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 Training Management System (TMS). Contractors will have access to this system for development purposes. All contractors are cleared using the VA background investigation process and must obtain a Minimum Background Investigation (MBI). Our Providers and Site Assistance components employ the same security mechanisms.

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 privacy and security training directives, courses and auditing apply, ensuring individual who have access to PII/PHI are trained to handle it appropriately. All individuals must complete all required VA TMS training for Privacy and HIPAA before being onboarded to the contract. The training records are retained for 7 years. This documentation and monitoring is performed through the use of the TMS.

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.***

Yes.

1. The Security Plan Status, Approved

2. The Security Plan Status Date, 16-Nov-2021

3. The Authorization Status, Authorization to Operate (ATO)

4. The Authorization Date, 27-Jan-2022

5. The Authorization Termination Date, 07-Aug-2023

6. The Risk Review Completion Date, 12-Jan-2022

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.

Yes, the system uses Salesforce Government Cloud Plus, which is a SaaS/PaaS offering with a FedRAMP High authorization.

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.

Yes, section 2.2 of Salesforce's Master Subscription Agreement states that all customer data will be deleted or destroyed from all systems 30 days after the effective date of contract termination.

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.

Yes, the full details are available on Salesforce.com's Privacy Statement.

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.

Yes, the VA and its contractors are ultimately responsible for the secure setup and configuration of the CSP's sharing, visibility, and general user access configuration. For example, the VA's configurations are what allow VAHC CRM to be only accessible to PIV authenticated users on the VA network.

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).

Not applicable.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Phillip Cauthers 255139 Digitally signed by Phillip Cauthers 255139
Date: 2023.01.04 12:32:19 -08'00'

Privacy Officer, Phillip Cauthers

JAMES BORING Digitally signed by JAMES BORING
Date: 2022.11.21 10:10:40 -05'00'

Information System Security Officer, James Boring

Michael S. Domanski 326889 Digitally signed by Michael S. Domanski 326889
Date: 2022.11.21 09:52:35 -05'00'

Information System Owner, Michael Domanski

APPENDIX A-6.1

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

System of Record Notice (SORN) 168VA005 Health Information Exchange-VA
https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf

VA Notice of Privacy Practices (NOPP) IB 10-163: https://www.va.gov/files/2022-02/Notice_of_Privacy_Practices_IB_10-163.pdf