Privacy Impact Assessment for the VA IT System called:

VA Health Connect Customer Relationship Management

(VAHC CRM)

Veterans Health Administration (VHA)

Office of Integrated Veteran Care (IVC)

eMASS#1926

Date PIA submitted for review: 12/16/2024

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 for VA?".

Through the VA Health Connect Customer Relationship Management (VAHC CRM) (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 Privacy Impact Assessment (PIA). A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 *General Description*

A. *What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*
The VA Health Connect Customer Relationship Management (VAHC CRM) tool, sponsored by the VHA Office of Integrated Veteran Care (IVC), 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.

B. *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*
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.

2. Information Collection and Sharing

C. *Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*
Current count is approximately 12,500,000. These records represent VHA Patient/Veteran population.

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

D. *What is a general description of the information in the IT system and the purpose for collecting this information?*
VHA Patient contact, enrollment, and health information for the purpose of delivering health care to Veteran patients.

E. *What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.*
VAHC CRM has three components:

- CRM – Currently the most used component for Registered Nurses, Medical Providers, Medical Support Assistants, Pharmacists, and Pharmacy Technicians. This component is considered the base or "core" functionality of VAHC from with other components can extend.
- Tele-EC Tracker – Used only by Emergency Care medical providers, this component was previously referred to "Tele-Urgent Care." Tele-EC Tracker provides similar capabilities such tracking workload and integration VistA, MPI, etc; however, this component is only used by the Emergency Medicine persona.
- Provider Connect – This component facilities a quick consultation between clinicians within the system.

F. Are the modules/subsystems only applicable if information is shared?

Yes, the modules/subsystems are applicable because the systems receive, store, and share data with one other to form a unified VA Health Connect system.

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

There is a singular, unified system that is accessible from various VA locations.

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

H. *What is the citation of the legal authority and SORN to operate the IT system?*

VAHC CRM is authorized to operate per legal authority, public law 113-146, Veterans Access, Choice, and Accountability Act of 2014.

H. *What is the SORN?*

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.

I. *SORN revisions/modification*

None.

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.*

The applicable SORNs do not required revision at this time.

4. System Changes

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

☐ *Yes*
☒ *No*

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

☐ *Yes*
☒ *No*

Section 1. Characterization of the Information

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

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

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

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

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

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

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

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

Other PII/PHI data elements: VistA local Patient Identifier (PatientLocalPid); VA Employee Data: Job Title, Email Address, VA User Security Identifier (SecId), Name, Author Designated User Id (DUZ)

1.2 List the sources of the information in the system

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

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

The data is coming from authoritative VA Data Sources: Master Person Index (MPI) and VA Profile. Updates to VA Profile information may be requested by the Veteran (or authorized caregiver/Power of Attorney) after successful verification and then entered into the system by the VAHC CRM clinical contact center user.

Other VA systems display data in real-time, however this data is not stored within the VAHC CRM system.

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

No commercial or public data is used.

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

No.

1.3 Methods of information collection

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

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

There are no web forms or other similar technology where information is captured from individuals. All information is collected from other VA systems through secure electronic transmission.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

Not applicable, as no information is collected on form.

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

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

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your

organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.
VAHC CRM system is not an authoritative data source; rather, it is integrated with VA Systems of Record (such as VA Profile, MPI, and VistA) and the data from these authoritative systems is displayed to the VAHC CRM users in real-time.

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

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?
No.

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

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

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.

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: VAHC CRM stores sensitive Veterans' PII and PHI. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal and financial harm to the individuals impacted and adverse negative effect to the VA.

Mitigation: 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 that will be used in support of the program's business purpose.

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

PII/PHI Data Element	Internal Use	External Use
Name	Identification purposes	Not used
Social Security Number	Identification purposes	Not used
Date of Birth	Identification purposes	Not used
Date of Death	Identification purposes	Not used
Mother's Maiden Name	Identification purposes	Not used
Mailing Address	Identification purposes	Not used
Personal Mailing Address	Identification purposes	Not used
Personal Phone Number	Identification purposes	Not used
Personal Email Address	Identification purposes	Not used
Emergency Contact Information	Identification purposes	Not used
Health Insurance Beneficiary Numbers	Identification purposes	Not used
Current Medications	Used for healthcare administration	Not used
Medical Records	Used for healthcare administration	Not used
Race/Ethnicity	Used for healthcare administration	Not used
Medical Record Number	Identification	Not used
Gender	Used for healthcare administration	Not used
Integrated Control Number (ICN)	Identification purposes	Not used
Military History/Service Connection	Identification purposes	Not used
Next of Kin	Identification purposes	Not used
VistA local Patient Identifier (PatientLocalPid)	Used for healthcare administration	Not used
Author DUZ (VA User's Author Designated User Id)	Used for healthcare administration	Not used
Department of Defense Identification Number (EDIPI)	Used for healthcare administration	Not used

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

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex

analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?
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.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
VAHC CRM will create a new Progress Note and/or Encounter record related to an existing Veteran's Electronic Health Record based on the information provided during the virtual call or visit. VAHC CRM may also update Veteran contact information such as (address, phone, and email) at the request of the Veteran or their authorized designee. The information can be made available to requestors by following the VA's standard procedures for requesting such access. Determinations are not made based on health data generated, as it is protected by the Health Insurance Portability and Accountability Act (HIPAA).

2.3 How the information in the system is secured.

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

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

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

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

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

2.4a How is access to the PII determined?

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.

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

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 (in accordance with VA Directive 6500), users are taught not to arbitrarily share data with co-workers unless the co-worker has a need for that data.

2.4c Does access require manager approval?

Anyone needing access to VAHC CRM 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.

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

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.

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

The VA Digital Transformation Center (DTC) is responsible for the production administration of the application.

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, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Phone Numbers, Personal Fax Number, Personal Email Address, Emergency Contact Information, Health Insurance Beneficiary Numbers, Medications, Medical Records, Race/Ethnicity, Medical Record Number, Gender, Integrated Control Number (ICN), Military History/Service Connection, Next of Kin, VistA local Patient Identifier (PatientLocalPid), Department of Defense Identification Number (EDIPI).

3.2 How long is information retained?

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

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

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

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

VAHC CRM follows the NARA Records Schedule DAA-0015-2017-0001 that was established for Department of Veterans Affairs Veterans Health Administration Call Centers. A link to the NARA Records Schedule is available at this link: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-veterans-affairs/rg-0015/daa-0015-2017-0001_sf115.pdf

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

VAHC CRM follows 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 or transfer of SPI?

Explain how records are destroyed, eliminated, or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.
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 VA Office of Information Security (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. 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. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

Privacy Risk: VAHC CRM stores sensitive Veteran PII and PHI. There is a risk that information may 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, breached, or exploited for reasons other than what is described in the privacy documentation associated with the information.

Mitigation: Information is maintained only as long as is required. 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.

PII Mapping of Components

4.1a Veterans Administration Health Connect CRM consists of one key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Veterans Administration Health Connect CRM and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/ No)	Does this system store PII? (Yes/ No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VAHC CRM Salesforce.com Database found at Salesforce.com (https://va-vet.my.salesforce.com [Production environment]; https://va-vet--perf.my.sandbox.salesforce.com [Pre-Production environment])	Yes	Yes	Veteran Data: SSN, DOB, Name, Gender, Phone, Mailing Address, Residential Address, Email Address, Mother's Maiden Name, Next of Kin, Emergency Contact	Required to enable functionality of system to allows users to appropriate identify Veterans and update their contact information if outdated.	Traffic is encrypted via TLS 1.2. System access is restricted to VA Network IP ranges. User login access required VA PIV/PIN multifactor authentication. Role-based access controls are configured to ensure principles of least-privilege.

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

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

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

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

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

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

Data Shared with Internal Organizations

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Corporate Data Warehouse (CDW)	Reporting & Analytics; system configuration data to facilitate workflows.	Name, SSN, ICN, Personal Phone Number(s), Personal Mailing Address, VistA local Patient Identifier (PatientLocalPid), Author b (VA User's Designated User Id).	Site to Site Encrypted with TLS 1.2
Cisco Finesse Telephony Servers	Integrates telephone with CRM to add efficiency.	Personal Phone Number(s)	Site to Site Encrypted with TLS 1.2
DTC Integration Platform (DIP)	Middleware to orchestrate API calls to other systems; no data is stored within this system.	Veterans or Dependents: Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Health Insurance Beneficiary Numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Gender, Integration Control Number (ICN), Military History/Service	Site to Site Encrypted with TLS 1.2

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
		Connection, Next of Kin, Name, PatientLocalPid, PatientLocalSiteId, VistA Identifier VA Employees: VistA Local Patient Identifier (PatientLocalPid) and corresponding VistA instance, Job Title, Email Address, VA User Security Identifier (SecId), SiteCode, ProviderName, Author Name, Job title, Author Designated User Id (DUZ)	
Digital Veterans Platform (DVP)	Address Validation Service	Veteran mailing and residential addresses	Site to Site Encrypted with TLS 1.2
eGain VA Knowledge Base	VA's Knowledge Base	No PHI or PII	Site to Site Encrypted with TLS 1.2
Eligibility & Enrollment System (ESR)	Displays registration status, insurance, and service connected information.	Veteran's Service branches, eligibilities, disability percentage, insurance, health benefit plans.	Site to Site Encrypted with TLS 1.2
Health Data Repository (HDR)	Displays clinical information from VistA.	Veteran's Clinical data for Consults, Flags, Medications, Progress Notes, Orders, Problems List, Radiology Exams, Visits, Vitals, Discharge Summaries, Immunizations, and allergies/adverse reactions.	Site to Site Encrypted with TLS 1.2
Master Person Index (MPI)	Authoritative Data Source for Person Information.	Veteran Data: Name, state of birth, country of birth, Personal Mailing Address, phone, date of death, Gender, SSN, VA User Security Identifier (SecId), and Department of Defense Identification Number (DoD EDIPI)	Site to Site Encrypted with TLS 1.2
Primary Care Management Module (PCMM)	Displays the VA and non VA providers that comprise the care team of a given Veteran patient.	VA Employees: Name, job titles, phone of the Patient Aligned Care Team (PACT) team members	Site to Site Encrypted with TLS 1.2
Triage Expert – Contact Center	Used as a triage tool based on symptoms.	Gender and Date of Birth	Site to Site Encrypted with TLS 1.2
VA Profile	Authoritative system for contact information such as phone, address, and email.	Veteran's Personal Mailing Address, Personal Phone Number(s), and Personal Email Address.	Site to Site Encrypted with TLS 1.2
Veterans Data Integration and Federation (VDIF)	Used to send Progress Notes into VistA.	VistA local Patient Identifier (PatientLocalPid), Progress Note Text, Clinic Location, Procedure	Site to Site Encrypted with TLS 1.2

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
		Codes, Diagnoses Codes, Visit RelatedTos), Author DUZ, Progress Note Title, Encounter String, Progress Note Text, eSignature, Clinic Location, Encounter Comments, Service Category, Procedure Codes, Diagnoses Codes, Visit RelatedTos)	
VistA	Used for healthcare delivery.	VA Employee Data: Internal VA Employee VistA designated user identifier and corresponding VistA local Patient Identifier (PatientLocalPid), Author DUZ (VA User's Author Designated User Id)	Site to Site Encrypted with TLS 1.2
Data Access Services (DAS)	Used to send Progress Notes into VistA.	Progress Notes (Site Code, Provider Name, Patient Name, Patient Local Pid, Patient Local Site Id, Author Name, Author DUZ, Progress Note Title, Encounter String, Progress Note Text, eSignature, Clinic Location, Encounter Comments, Service Category, Procedure Codes, Diagnoses Codes, Visit RelatedTos)	Site to Site Encrypted with TLS 1.2
EAS Enterprise Appointment Service (EAS)	VistA scheduling application	Appointment request comments, appointment comments, ICN, Veteran Mobile Phone Number, Veteran Email Address	Site to Site Encrypted with TLS 1.2
ClearTriage	Decision support tool	Not applicable; there is no PII or PHI shared with this system.	Site to Site Encrypted with TLS 1.2
Entra Id (iDaas)	Parallel Path for authentication	VA Employee Data: Integrated Control Number (ICN), Internal VA Employee VistA Id	Site to Site Encrypted with TLS 1.2
Federal EHRM (Oracle Health)	Oracle Cerner Data bidirectional using DAS middleware. This will send PHI/PII counters on progress notes similar to HDR.	Veteran's Clinical data for Consults, Flags, Medications, Progress Notes, Orders, Problems List, Radiology Exams, Visits, Vitals, Discharge Summaries, Immunizations, and allergies/adverse reactions; Integrated Control Number (ICN), and Department of Defense Identification Number (EDIPI).	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 VA network and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions in this section.).

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

Follow the format below:

Privacy Risk: Data sharing is necessary for VHA to provide care to Veterans. There is risk data could be shared with inappropriate organizations or institutions which has the potential for loss of information due to theft or destruction with the shared information.

Mitigation: Safeguards are implemented to ensure data is not inappropriately shared or accessed. 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 the United States Privacy Act of 1974, 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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

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

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

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

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

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

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

Data Shared with External Organizations

List IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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

Follow the format below:

Privacy Risk: There is no external sharing.

Mitigation: There is no external sharing.

Section 6. Notice

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

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

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

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

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

SORN 24VA10A7 Patient Medical Records–VA:.
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf.

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.

SORN 168VA005 Health Information Exchange-VA: https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf.

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

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

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.
Please see the detailed content of the notices identified in the response to question 6.1a above.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.
Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.
Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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

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

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

Principle of Use Limitation: *The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must ensure that information is used only for the purpose articulated in the notice.*
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:
Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records. The NOPP is also available at all VHA medical centers from the facility Privacy Officer.

The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

Section 7. Access, Redress, and Correction

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

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

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

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

There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office.

VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access.VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

The system is not exempt from the Privacy Act.

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

The system is not exempt from the Privacy Act.

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

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SORN. Every Privacy Act SORN contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) which states:

Right to Request Amendment of Health Information.

You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.
If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights.

In response, you may do any of the following:

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

Individuals seeking information regarding access to and contesting of VA benefits records may write, call or visit the nearest VA regional office.

Additional notice is provided through the SORS listed in 6.1 of this PIA and through the Release of Information Office where care is received.

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. ***<u>Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.</u>***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.
Formal redress via the amendment process is available to all individuals, as stated in questions 7.1-7.3.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

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

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

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

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

Follow the format below:

<u>Privacy Risk:</u> There is a risk that a Veteran/caregiver will not know the relevant procedures for gaining access to, correcting, or contesting their information in VAHC CRM.

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

The Release of Information (ROI) office at a VA medical center is available to assist Veterans with obtaining access to their health records and other records containing personal information. The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

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

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

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

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

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?
Users from other agencies do not have access to VAHC CRM.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.
Medical Providers, Pharmacists, Clinical Triage Nurses, Medical Support Assistants, TeleEC Supervisors, TeleEC Medical Providers, and Provider Connect users comprise the major roles within the system. Each of these personas have specific edit access for pertinent fields relevant to their persona. In addition to field-level security, there is also record-level security such that a medical support assistant cannot create a Pharmacy progress note, for example.

8.2a. Will VA contractors have access to the system and the PII?

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 Booz Allen 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.

8.2b. What involvement will contractors have with the design and maintenance of the system?
Contractors are responsible for the technical implementation and maintenance of the system based on requirements provided by VHA and OIT.

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

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

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?
If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.
Yes, all contractors with access are required to take annual VA Privacy training and complete an electronic elevated privileges access request that is approved by the COR.

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 are performed through the use of the TMS

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date: 05/26/2023*
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 07-25-2023
5. *The Authorization Termination Date:* 07-24-2025
6. *The Risk Review Completion Date:* 12-July-2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* HIGH

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***
Not applicable.

Section 9 – Technology Usage

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

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

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

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

VA owns the data. Additionally, 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.

https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/salesforce_MSA.pdf

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

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

Ancillary Data, as described in NIST 800-144, is collected automatically the CSP but owned by the Department of Veterans Affairs.

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).* The system does not utilize Robotics Process automation (RPA).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

PHILLIP CAUTHERS

Digitally signed by PHILLIP CAUTHERS
Date: 2025.02.03 09:12:24 -08'00'

Privacy Officer, Phillip Cauthers

JAMES BORING

Digitally signed by JAMES BORING
Date: 2025.01.29 10:40:39 -05'00'

Information System Security Officer, James Boring

MICHAEL DOMANSKI

Digitally signed by MICHAEL DOMANSKI
Date: 2025.01.29 09:27:12 -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; screen shot of a website collection privacy notice).

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

SORN 24VA10A7 Patient Medical Records–VA:.
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf.

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.

SORN 168VA005 Health Information Exchange-VA: https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf.

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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

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

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

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

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=11693

VA Notice of Privacy Practices: IB 10-163p (va.gov)