Privacy Impact Assessment for the VA IT System called:

Community Care Referral and Authorization (CCRA) System Assessing

Veteran Health Administration (VHA)

Integrated Veteran Care (IVC)

eMASS ID #760

Date PIA submitted for review:

January 3, 2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Eller Pamintuan	Eller.pamintuan@va.gov	303-331-7512
Information System Security Officer (ISSO)	Kimberly Keene	kimberly.keene@va.gov	703-441-3063
Information System Owner	Dena Liston	dena.liston@va.gov	202-603-4493

Abstract

The abstract provides the simplest explanation for "what does the system do for VA?".

Community Care Referral and Authorization (CCRA) System Assessing is an enterprise-wide system used by communication care staff to generate referrals and authorization for Veterans receiving care in the community. Clinical and Department of Veterans Affairs (VA) community care staff located at VA medical centers (VAMCs), outpatient clinics, community-based outpatient clinics (CBOCs), and Veterans Integrated Service Network (VISN) office use this solution to enhance Veteran access to care. CCRA System Assessing is an integral component of community care information technology (IT) architecture that allows Veterans to receive care from community providers.

CCRA System Assessing has allowed VA to transition from a largely manual process to a more streamlined process that generates standardized referrals and authorizations according to clinical and business rules. CCRA System Assessing supports clinical and administrative processes that:

- Seamlessly provide eligible Veterans with prompt referrals to a community provider of their choice
- Provide community providers with referrals and authorizations consistent with industry standards
- Decrease the administrative burden on VA clinical and facility community care staff members by establishing clinical and business pathways that reflect best practices, consistent outcomes, and reduced turnaround times, along with solution that automates those pathways.
- Facilitate communication between facility community care staff and community providers via a unified platform that enables the secure exchange of medical information.

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?

CCRA System Assessing provides support to Veterans Health Administration (VHA) and gives securely managed access to 125,000+ users nation-wide, including VA staff, external providers, claims processors, and others. CCRA System Assessing provides a unified user experience enabled with single sign on for ease of use. The Intuitive Reliable Interoperative Scalable (IRIS) for Health platform is used for all connectivity between our solutions and all

VA and external systems. IRIS for Health provides the capacity to deal with legacy connections based on Health Level 7 (HL7), Secure File Transfer Protocol (SFTP) and Simple Mail Transfer Protocol (SMTP), as well as more modern approaches like Representational State Transfer (REST) and Fast Healthcare Interoperability Resources (FHIR). Leveraging this capacity has allowed the system to maintain and manage connectivity to more than 25 VA enterprise systems.

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.*

CCRA System Assessing is owned and operated by VA.

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?*

All Veterans and dependents eligible for care through community providers and referred to a community provider are within the CCRA System Assessing applications. CCRA System Assessing has managed referral and appointment information for over 1.5 million unique veterans.

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?*

CCRA System Assessing automatically generates referrals and authorizations for all Veterans receiving care in the community and contains personally identifiable information (PII) and protected health information (PHI).

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

CCRA System Assessing receives data gathered from VA systems and does not include information collected directly from an individual or Veteran. Specific interconnections, both internal and external, with VA are defined within Section 4 and Section 5.

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

Yes, modules and subsystems for CCRA System Assessing are only applicable if information is shared.

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?*

CCRA System Assessing is a web-based system hosted in the AWS GovCloud.

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?*

CCRA System Assessing is an enterprise-wide solution in support of the Veterans Access, Choice, and Accountability Act of 2014 (Pub. L. 113-146) ("Choice Act"), as amended by the VA Expiring Authorities Act of 2014 (Pub. L. 113-175), to generate referrals and authorizations for Veterans receiving care in the community. VA clinical providers and non-VA clinical providers access a cloud-based software system to request and refer clinical care for Veterans with community care providers. This solution enhances Veteran access to care by using a common and modern system to orchestrate the complex business of VA referral management.

H. *What is the SORN?*

The CCRA System Assessing SORN is SORN 180VA10D HealthShare Referral Manager (HSRM)-VA.

I. *SORN revisions/modification*

No revisions or modifications to the SORN are required.

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

No revisions or modifications to the SORN are required.

4. System Changes

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

☐ Yes
☒ No
if yes, N/A

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

☐ Yes
☒ No
if yes, N/A

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

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

☒ 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)

Other PII/PHI data elements:

- Residential Address
- Data File Number (DFN)
- Veterans Choice Eligibility
- Enrollment and Eligibility Status
- Service-Connected Disability
- Provisional Diagnosis
- Category of Care
- Services Requested
- Appointment Information
- Community Care Clinical Coordination Contact Center (C6) Provider Designation

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?

CCRA System Assessing receives data gathered from VA systems and does not include information collected directly from an individual or Veteran. Specific interconnections with VA are defined within Section 4.

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.

CCRA System Assessing receives and uses data from other VA systems of record, which are defined within Section 4.

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

CCRA System Assessing only creates and manages patient appointment information.

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?

CCRA System Assessing receives data gathered from VA systems and does not include information collected directly from an individual or Veteran. Specific interconnections with VA are defined within Section 4. All information is delivered to CCRA System Assessing electronically using various forms of technology, including HL7 messaging, JavaScript Object Notation (JSON), and extensible markup language (XML) over REST(ful) and Simple Object Access Protocol (SOAP). VA provided source data, is transmitted via VA network or VA employee verified and entered.

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?

CCRA System Assessing receives data gathered from VA systems and does not include information collected directly from an individual or Veteran. Specific interconnections with VA are defined within Section 4. VA provided source data, is transmitted via VA network or VA employee verified and entered.

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.

Data received and maintained by CCRA System Assessing is checked against any other source of information (within Integrated Veteran Care [IVC]) before the information is received or used to make decisions about an individual. Data that cannot be automatically verified through VA network connections are VA employee verified utilizing data within VA systems instead of CCRA System Assessing.

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?

Data that cannot be automatically verified through VA network connections are VA employee verified utilizing data within VA systems instead of CCRA System Assessing.

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

The legal authorities covering the CCRA System Assessing use of PHI and PII for medical care are as follows:

- Veterans Access Choice and Accountability Act (VACAA) (Public Law 113–146)
- Amendment to VACAA (Public Law 115-26)
- Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191)
- Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations (45 C.F.R. 164.506)
- 38 U.S.C. Coordination and Promotion of Other Programs Affecting Veterans and Their Dependents, Section 523(a), 6301-6307, section 7301(a) 8111, 8153
- 10 U.S.C. 1104, Sharing of Health Care Resources with the Department of Veterans Affairs
- 26 U.S.C. Internal Revenue Code, 61(a), Gross Income Defined
- 26 U.S.C. 31, Employment Taxes and Collection of Income Tax at Source
- 26 U.S.C. 1741–1743 Criteria for Payment
- 28 U.S.C. 1781, Transmittal of Letter Rogatory or Requests
- 42 U.S.C. 1786, Special Supplemental Nutrition Program for Women, Infants, and Children (WIC)
- 8 U.S.C. 1787 – Health Care of Family Members of Veterans stationed at Camp Lejeune, North Carolina
- 38 U.S.C. 3102, Basic Entitlement
- 38, U.S.C. 5701 Confidential Nature of Claims
- 5 U.S.C. Travel and Transportation Expenses of Employees Transferred; Advancement of Funds; Reimbursement on Commuted Basis
- 38 U.S.C. 7332 Confidentiality of Certain Medical Records
- 18 U.S.C. 1831, Economic Espionage,
- 45 C.F.R. Part 160, subpart B, Emergency Board
- Title 44 U.S.C. Public Printing and Documents
- Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014
- Title 38 U.S.C. 1703 – Veterans Community Care Program; Veterans Access, Choice, and Accountability Act of 2014 (Pub. L. 113–146).
- Title 38, U.S.C. Section 501(a), Rules and Regulations
- Title 38, U.S.C. Section 1705, Management of Health Care: Patient Enrollment System,
- Title 38, U.S.C. Section 1710, Eligibility for Hospital, Nursing Home, and Domiciliary Care,
- Title 38, U.S.C. Section 1722, Determination of Inability to Defray Necessary

Expenses; Income Thresholds,

- Title 38, U.S.C. Section 1781, Medical Care for Survivors and Dependents of Certain Veterans
- Title 5, U.S.C. Section 552(a), Public Information; Agency Rules, Opinions, Orders, Records, and Proceedings

SORN routine use Title 44 U.S.C. Applicable SORNs include:

- 23VA10NB3, Non-VA Care (Fee) Records-VA, published July 30, 2015
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA, published March 3, 2015
- 155VA10, Customer Relationship Management System (CRMS) – VA published September 15, 2023
- 180VA10D, HealthShare Referral Manager (HSRM) – VA, published August 17, 2021

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

Principle of Purpose Specification: 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: CCRA System Assessing contains Sensitive Personal Information (SPI), including SSNs, names, and PHI. Due to the nature of this data, there is a risk that if the data were accessed by an unauthorized individual, or otherwise breached, identity theft or other serious harm could occur.

Mitigation: CCRA System Assessing uses commercial off-the-shelf (COTS) product known as HSRM that is hosted in an AWS GovCloud authorized under the Federal Risk and Authorization

Management Program (FedRAMP) at the high-impact level. The system is monitored for unusual activity using automated and manual tools, and abnormal activity is immediately addressed.

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	Identify the Veteran	Identify the Veteran
SSN	Identify the Veteran	Identify the Veteran
DOB	Determine the Veteran's age, inform community care providers, and to support medical treatment and decision-making	Determine the Veteran's age, inform community care providers, and to support medical treatment and decision-making
Residential Address	Determine nearest community provider for care	Determine nearest community provider for care
Mailing Address	Facilitate communication	Facilitate communication
Phone Number(s)	Facilitate communication	Facilitate communication
Race/Ethnicity	Inform community providers, support medical treatment, and decision making	Inform community providers, support medical treatment, and decision making
ICN	Identify the Veteran	Identify the Veteran
DFN	Identify the Veteran	Identify the Veteran
EDIPI	Identify the Veteran	Identify the Veteran
Email	Veteran Notification	Veteran Notification
Gender	Inform community providers, support medical treatment, and decision making	Inform community providers, support medical treatment, and decision making
Medication	Inform community providers, support medical treatment, and decision making	Inform community providers, support medical treatment, and decision making
Medical Records	Inform community providers, support medical treatment, and decision making	Inform community providers, support medical treatment, and decision making
Health Insurance Beneficiary Numbers	Determine qualification of benefits including health care	Determine qualification of benefits including health care
Beneficiary Type	Determine qualification of benefits including health care	Determine qualification of benefits including health care

PII/PHI Data Element	Internal Use	External Use
Veterans Choice Eligibility	Indicate approval for a Veteran to receive specific medical care by a community provider and ensure VA will pay for the authorized non-VA services	Indicate approval for a Veteran to receive specific medical care by a community provider and ensure VA will pay for the authorized non-VA services
Service-Connected Disability	Disability Qualification	Disability Qualification
Provisional Diagnosis	Determine care and treatment required	Determine care and treatment required
Category of Care	Determine care and treatment required	Determine care and treatment required
Services Requested	Determine care and treatment required	Determine care and treatment required
Appointment Information	Determine care and treatment required	Determine care and treatment required
C6 Provider Designation	Determine care and treatment required	Determine care and treatment required

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?

CCRA System Assessing uses built-in reporting tools to analyze data. This tool is used for aggregation and filtering, and statistical reports and not for novel findings. CCRA System Assessing allows community providers to upload documents containing any data that they choose. These documents are subsequently moved to more appropriate locations via a task assignment 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.

Information is made available for VA within the CCRA System Assessing applications to allocate care in the community. A new referral is created against an existing patient’s record.

Information is used by VAMCs to make community provider appointments for the Veteran's medical care.

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?

CCRA System Assessing data is encrypted at rest and in transit. SSNs are encrypted and masked via the CCRA System Assessing application interface and other PII and PHI details are protected based on access to the application and the "need to know" basis.

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).

CCRA System Assessing encrypts and stores only the last four digits of an SSN, this information is available to select approved and provisioned users as required for the proper performance of their duties.

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

CCRA System Assessing employees and subcontractors sign the Contractor Rules of Behavior (CROB) when hired and annually following privacy and security trainings within VA Talent Management System (TMS).

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

Principle of Transparency: 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.

2.4a How is access to the PII determined?

Access to PII is limited by role assignment, which is completed in one of two ways:

- Option 1: Roles are assigned via the same user process and list as provisioning below, where roles can be provided and loaded into the system.
- Option 2: A manual process is employed via a help desk call with the same process and caveats as above, local IT for single sign-on internal (SSOi) and for single sign-on external (SSOe).

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?

Criteria, procedures, controls, and responsibilities are defined in the CCRA System Assessing End User Secure Access Management Plan. Access requires manager approval. The HSRM Service Desk receives communications from the end user staff management to create an account via the Enterprise Service Desk (ESD) ticketing process. Upon notification from the applicable trainer that the user has successfully completed the HIPAA/security awareness, privacy and security, and compliance training, the Service Desk creates the user's account, including username, role, and dashboard, in accordance with Cognosante Access Control Policies and Procedures.

2.4c Does access require manager approval?

The request is initiated by the user's direct supervisor and approved within ServiceNow or by the Project Management Office (PMO) and approved by the project's Sr. Program Manager for CCRA System Assessing. The email contains the position requirements and role of the end user, which outlines the user's hire date and role specifications.

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

Access and changes to data, including PII/PHI is monitored within HSRM using built in audit logs capability.

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

The CCRA System Assessing Security and Privacy Officer and ISO are responsibility for safeguarding the security and privacy of VA data within eMASS.

Section 3. Retention of Information

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

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is ***retained*** *by the system.*

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

The information retained by CCRA System Assessing includes Name, SSN, DOB, Residential and Mailing Address, Phone Number(s), Health Insurance (Beneficiary Numbers, Account Numbers), Medications, Medical Records, Race/Ethnicity, EDIPI, ICN, DFN, TCN, Email, Gender, Veterans Choice Eligibility, Enrollment and Eligibility, Service-Connected Disability, Provisional Diagnosis, Category of Care, Services Requested, Appointment Information, and C6 Provider Designation.

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.*

CCRA System Assessing collects information to referrals and relies on information in AWS GovCloud and the interconnections defined within Section 4 to retain data. The data is retained as part of the individual's health care record and is retained according to the rules applied to those records.

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?

Yes, CCRA System Assessing follows VA Records Control Schedule (RCS) 10-1 for record retention and disposal guidance. Reference VA RCS 10-1 for further details at this link: [https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf.](https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf)

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

Referrals begin at the VAMC and are maintained in the medical files for 75 years after last episode of care. Working records that go to CCRA System Assessing are temporary 3 years after last episode of care). At the conclusion of care, the records are returned to the VAMC for retention.

The information retained by CCRA System Assessing applications is listed in Section 3.1. Feeder records are original records and are maintained in accordance with the policies of AWS GovCloud and the interconnections defined in Section 4.

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.

CCRA System Assessing relies on information from the interconnections defined in Section 4 and only collects information related to referrals. All data is retained as part of the individual's health care record and is retained according to the rules applied to those records.

Referrals begin at the VAMC and are maintained in the medical files for 75 years after last episode of care. Working records that go to CCRA System Assessing are temporary 3 years after last episode of care). At the conclusion of care, the records are returned to the VAMC for retention.

The information retained by CCRA System Assessing applications is listed in Section 3.1. Feeder records are original records and are maintained in accordance with the policies of AWS GovCloud and the interconnections defined in Section 4.

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.

CCRA System Assessing does not use real data for development, research, testing or training.

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

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (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: Increased risk of exposure of records are retained longer than the designated retention period.

Mitigation: CCRA System Assessing follows VHA RCS 10-1 and all records are retained based on what is outlined in VHA RCS 10-1. When it is time for dissemination, CCRA System Assessing follows the steps listed in **3.4**.

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 CCRA System Assessing consists of 106 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 CCRA System Assessing 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
CCRA	Yes	Yes	Name, SSN, DOB, Residential and Mailing Address, Phone Number(s), Health Insurance (Beneficiary Numbers, Account Numbers), Current Medications, Previous Medical Records, Race/Ethnicity, EDIPI, ICN, DFN, Email, Gender, Beneficiary Type, Veterans Choice Eligibility, Provisional Diagnosis, Category of Care, Services Requested, Appointment Information	Data used by community care staff to generate referrals and authorization for Veterans receiving care in the community	Data in transit is secured using Transport Layer Security (TLS) and Secure File Transport Protocol (SFTP). Data is encrypted at rest.

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***
Cerner	Receive Community Care Consults	Name, SSN, DOB, Residential and Mailing Address, Phone Number(s), Race/Ethnicity, EDIPI, ICN, DFN, Email, Gender, Provisional Diagnosis, Category of Care, Services Requested	Transmitted via HL7 messages from Cerner
Community Care Reimbursement System (CCRS)	Send referral information so that Community Care Third Party Payors can be Reimbursed	Name, SSN, DOB, Residential and Mailing Address, Phone Number(s), Health Insurance (Beneficiary Numbers, Account Numbers), Race/Ethnicity, Email, Gender, Beneficiary Type	Transmitted via SFTP within the VA network, files at rest are encrypted; HSRM consumes the information CCRS provides

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)	Referral data to be housed in the corporate data warehouse	Name, SSN, DOB, Residential and Mailing Address, Phone Number(s), Health Insurance (Beneficiary Numbers, Account Numbers), Race/Ethnicity, Email, Gender, Beneficiary Type	Transmitted to CDW from the various SQL databases using HTTPS
Data Access Service (DAS)	Referrals are transmitted through DAS to be sent to TPA	Name, SSN, DOB, Residential and Mailing Address, Phone Number(s), Health Insurance (Beneficiary Numbers, Account Numbers), Race/Ethnicity, Email, Gender, Beneficiary Type	Transmitted via a REST web service over HTTPS; DAS consumes the information HSRM provides
Electronic Claims Adjudication Management System (eCAMS)	Process out of network claims	Name, SSN, DOB, Residential and Mailing Address, Phone Number(s), Health Insurance (Beneficiary Numbers, Account Numbers), Race/Ethnicity, Email, Gender, Beneficiary Type	Transmitted via SFTP HTTPS; HSRM provides the information eCAMS consumes
Emergency Care Authorization Tool (ECAT)/Non-Contract Assessment Tool (NCAT)	Receive notifications of community emergency care and to process notifications for payment	Name, SSN, DOB, TCN, Residential and Mailing Address, Phone Number(s), Email, Gender, Enrollment and Eligibility Status, Suicidal Crisis Status, Medical Complaint, Admission and Discharge Diagnosis	TLS is encrypted in transit
Enrollment System (ES)	Evaluate eligibility for care in the community	Name, SSN, DOB, Residential and Mailing Address, Phone Number(s), Health Insurance (Beneficiary Numbers, Account Numbers), Race/Ethnicity, Email, Gender, Beneficiary Type	Transmitted via a SOAP web service over HTTPS; ES provides the information HSRM consumes

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***
Identity and Access Management (IAM) SSOe	Provides VA users access to HSRM and ECR	Email	Transmitted via SAML assertion passed as part of the redirect to the login page; HSRM consumes the information SSOe provides
IAM SSOi	Provides Community Providers access to HSRM	Email	Transmitted via SAML assertion passed as part of the redirect to the login page; HSRM consumes the information SSOi provides
Master Patient Index (MPI)	Update Veteran demographics	Name, SSN, DOB, Residential and Mailing Address, Phone Number(s), Gender	Transmitted via a SOAP web service over HTTPS
Payer Electronic Data Interchange (EDI) Transactions Application Suite (TAS)	Retrieve data to be shared with TPAs and providers	Name, SSN, Residential Address, ICN	Transmitted via a REST API over HTTPS
Patient Centered Management Module (PCMM)	Retrieve C6 provider designation	Name, C6 provider designation	Transmitted via a REST API over HTTPS
Program Integrity Tool (PIT)	Evaluate waste, fraud and abuse	Name, SSN, DOB, Residential and Mailing Address, Phone Number(s), Health Insurance (Beneficiary Numbers, Account Numbers), Race/Ethnicity, Email, Gender, Beneficiary Type	Transmitted via REST web service over HTTPS; HSRM provides the information PIT consumes

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***
Provider Profile Management System (PPMS)	Retrieve Community Provider information that may be associated to a referral	N/A	Transmitted via a REST web service over HTTPS; HSRM consumes the information PPMS provides
Veterans Affairs Online Scheduling (VAOS)	Retrieve scheduling information	Name, SSN, DOB, Residential and Mailing Address, Phone Number(s), ICN, DFN, Email, Gender	Transmitted via a REST web service over HTTPS
Veterans Data Integration and Federation (VDIF)	Provide VA and Community Providers access to view Veteran clinical data	Name, SSN, EDIPI, Gender	Transmitted via SOAP web services over HTTPS
Veterans Health Information Systems and Technology Architecture (VistA)	Receive Community Care Consults	Name, SSN, DOB, Residential and Mailing Address, Phone Number(s), Race/Ethnicity, EDIPI, ICN, DFN, Email, Gender	Transmitted via HL7 messages from HSRM which VistA consumes

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: PII may be accidently released to unauthorized individuals.

Mitigation: Information is only accessible to authorized individuals who gain access with their personal identification verification (PIV) card and providing a pin. All users must take HIPAA and VA Privacy and Security training. CCRA System Assessing follows National Institute of Standards and Technology (NIST) audit accountability standards, and VA Directive 6500, with audit logs monitored periodically.

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***
HSRM COTS Product		Name, SSN, DOB, Residential and Mailing Address, Phone Number(s), Health Insurance (Beneficiary Numbers, Account Numbers), Current Medications, Previous Medical Records, Race/Ethnicity, EDIPI, ICN, DFN, Email, Gender, Beneficiary Type, Veterans Choice Eligibility, Service-Connected Disability, Provisional Diagnosis, Category of Care, Services Requested, Appointment Information	Interconnection Security Agreement (ISA)/ Memorandum of Understanding (MOU)	Data is shared with external providers via HTTPS Data includes the minimum information specifics to the referral

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

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

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:

<u>Privacy Risk:</u> PII may be accidently released to unauthorized individuals.

<u>**Mitigation:**</u> Information is only accessible to authorized individuals who gain access with their approved SSOe-provided credentials and provide a password. All users must take HIPAA and VA privacy and security training. Audit logs are in place. For external users, ID.me is used for authentication and VA SSOe is used for authorization.

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.

CCRA System Assessing imports data from VA systems and does not include information collected directly from an individual or Veteran. Specific interconnections with VA are defined within Section 4. A notice is provided to individuals when data is collected for VistA or Cerner.

6.1b If notice was not provided, explain why.

CCRA System Assessing imports data from VA systems and does not include information collected directly from an individual or Veteran. Specific interconnections with VA are defined within Section 4. A notice is provided to individuals when data is collected for VistA or Cerner.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

Privacy notices are provided at the point of service at the medical center where the Veteran receive care, in accordance with VHA Handbook 1605.4, Notice of Privacy Practices. Notice of privacy practices are available on the https://www.va.gov/privacy/

Each of the above notices includes information on how to report any use of information that is not in accordance with the collection. Reference Error! Reference source not found.Notice of Privacy Practices link to the notice of privacy practices provided at all VAMCs.

System of records notices that apply to the collection, use and disclosure of information within this data collection are located at https://www.oprm.va.gov/privacy/systems_of_records.aspx.

- 23VA10NB3, Non-VA Care (Fee) Records – VA (July 30, 2015)
- 24VA10A7, Patient Medical Records – VA (October 12, 2020)
- 79VA10P, VistA Records – VA (December 23, 2020)
- 97VA10, Consolidated Data Information System – VA (December 23, 2020)
- 121VA1007, National Patient Databases – VA (February 12, 2018)
- 147VA10, Enrollment and Eligibility Records – VA (August 17, 2021)
- 180VA10D, HealthShare Referral Manager (HSRM) – VA (August 17, 2021)

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.

CCRA System Assessing imports data from VA systems and does not include information collected directly from an individual or Veteran. Specific interconnections with VA are defined within Section 4. A notice is provided to individuals when data is collected for VistA or Cerner.

Reference Error! Reference source not found.Notice of Privacy Practices for the complete notice. The notice states the following details for restrictions:

Right to Request Restriction. You may request that we not use or disclose all or part of your health information to carry out treatment, payment, or health care operations, or that we not use or disclose all or part of your health information with individuals such as your relatives or friends involved in your care, including use or disclosure for a particular purpose or to a particular person. Please be aware, that because VHA, and other health care organizations are “covered entities” under the law, VHA is not required to agree to such restriction, except in the case of a disclosure restricted under 45 CFR § 164.522(a)(1)(vi). This provision applies only if the disclosure of your health information is to a health plan for the purpose of payment or health care operations and your health information pertains solely to a health care service or visit which you paid out of pocket in full. However, VHA is not legally able to accept an out-of-pocket payment from a Veteran for the full cost of a health care service or visit. We are only able to accept payment from a Veteran for co-payments. Therefore, this provision does not apply to VHA and VHA is not required or able to agree to a restriction on the disclosure of your health information to a health plan for the purpose of receiving payment for health care services VA provided to you. To request a restriction, you must submit a written request that identifies the information you want restricted, when you want it to be restricted, and the extent of the restrictions. All requests to restrict use or disclosure should be submitted to the facility Privacy Officer at the VHA health care facility that provided or paid for your care. If we agree to your request, we will honor the restriction until you revoke it unless the information covered by the restriction is needed to provide you with emergency treatment or the restriction is terminated by VHA upon notification to you. NOTE: We are not able to honor requests to remove all or part of your health information from the electronic database of health information that is shared between VHA and DoD, or to restrict access to your health information by DoD providers with whom you have a treatment relationship.

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.

CCRA System Assessing imports data from VA systems and does not include information collected directly from an individual or Veteran. Specific interconnections with VA are defined within Section 4. A notice is provided to individuals when data is collected for VistA or Cerner.
Individuals have a right to contact the VHA Enterprise Service Desk (ESD) at 855-673-4357 to gain access to their information.

Reference Error! Reference source not found.Notice of Privacy Practices for the complete notice. The notice states the following details for authorization:

Other Uses and Disclosures with Your Authorization. We may use or disclose your health information for any purpose you specify in a signed, written authorization you provide us. Your signed, written authorization is always required to disclose your psychotherapy notes if they exist. If we were to use or disclose your health information for marketing purposes, we would require your signed written authorization. In all other cases, we will not use or make a disclosure of your health information without your signed, written authorization, unless the use or disclosure falls under one of the exceptions described in this Notice. When we receive your signed, written authorization we will review the authorization to determine if it is valid, and then disclose your health information as requested by you in the authorization.

Revocation of Authorization. If you provide us a signed, written authorization to use or disclose your health information, you may revoke that authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose your health information unless the use or disclosure falls under one of the exceptions described in this Notice or as otherwise permitted by other laws. Please understand that we are unable to take back any uses or disclosures we have already made based on your signed, written authorization.

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:

<u>Principle of Transparency:</u> This is referring to sufficient notice provided to the individual.

<u>Principle of Use Limitation:</u> 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:

<u>Privacy Risk:</u> If notice is not provided in a timely manner, an individual might give information that they do not want to be shared.

<u>Mitigation:</u> CCRA System Assessing collects no information from Veterans. Information in this system is gathered through other VA systems. Veteran and Beneficiaries are provided notice of Privacy Practices in and through several different locations before their information is collected. Reference Error! Reference source not found.Notice of Privacy Practices for the complete notice.

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 <u>VA Public Access Link-Home (efoia-host.com)</u> to obtain information about FOIA points of contact and information about agency FOIA processes.***

Error! Reference source not found.

Reference Error! Reference source not found.Notice of Privacy Practices for the complete notice. The notice states the following details for obtaining a copy of health information:

Right to Review and Obtain a Copy of Health Information. You have the right to review and obtain a copy of your health information in our records. You must submit a written request to the facility Privacy Officer at the VHA health care facility that provided or paid for your care. The VHA Privacy Office at Central Office in Washington, D.C. does not maintain VHA health records, nor past military service health records. For a copy of your military service health records, please contact the National Personnel Records Center at (314) 801-0800. The Web site is http://www.archives.gov/veterans/military-service-records/medical-records.html.

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)?

CCRA System Assessing application is not exempt. Reference Error! Reference source not found.Notice of Privacy Practices for the complete notice.

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?

Reference Error! Reference source not found.Notice of Privacy Practices for the complete notice. The notice states the following details for obtaining a copy of health information:

Right to Review and Obtain a Copy of Health Information. You have the right to review and obtain a copy of your health information in our records. You must submit a written request to the facility Privacy Officer at the VHA health care facility that provided or paid for your care. The VHA Privacy Office at Central Office in Washington, D.C. does not maintain VHA health records, nor past military service health records. For a copy of your military service health records, please contact the National Personnel Records Center at (314) 801-0800. The web site is http://www.archives.gov/veterans/military-service-records/medical-records.html.

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 have a right to contact the VHA call center at 855-673-4357 to gain access to their information. Reference Error! Reference source not found.Notice of Privacy Practices for the complete notice. The notice states the following details for obtaining a copy of health information:

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 or health 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.

> Individuals have a right to contact the VHA call center at 855-673-4357 to gain access to their information. Reference Error! Reference source not found.Notice of Privacy Practices for the complete notice. The notice states the following details for obtaining a copy of health information:
>
> 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 or health records.

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

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

> Individuals have a right to contact the VHA ESD at 855-673-4357 to gain access to their information.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

Principle of Individual Participation: 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.

Principle of Individual Participation: 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:

Privacy Risk: There is a risk information provided to CCRA System Assessing is incorrect resulting in false appointment information being displayed.

Mitigation: Individuals have a right to contact the VHA call center to gain access to their information. Disclosure of SSNs of those for whom benefits are claimed is requested under the authority of 38 U.S.C. and is voluntary. SSNs will be used in the administration of Veterans' benefits and in the identification of Veterans or persons claiming or receiving VA benefits and their records and may be used for other purposes where authorized by 38 U.S.C. and the Privacy Act of 1974 (5 U.S.C. 552a) or where required by other statutes.

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?

There are two access-provisioning mechanisms—one for internal VA employees and contractors and one for external health care providers. Both provisioning mechanisms are accomplished through IAM.

VA Internal Authentication, SSOi

The IAM SSOi service is an authentication service specifically designed for controlling access for VA internal users (employees and contractors) accessing VA applications. This service enhances the user experience by reducing the time associated with multiple logon and logoff activities that require application-specific identifiers and passwords. The service also enables enriched password management and reduction in help desk support.

CCRA System Assessing is integrated with the VA IAM SSOi for all internal user-facing VA applications, which provides two-factor authentication compliance. The VA PIV card provides the required second piece to the two-factor authentication. To achieve this authentication there is an SSOi SAML partnership in which the SSOi service is the identity provider, and the application is in the service provider role. SSOi uses a previously authenticated session user as the subject for this identity provider and generates a signed and encrypted new SAML token for the partner application to process.

Support for government-approved algorithms must be provided (e.g., signature: rsa-sha256 and encryption: AES256).

External Authentication, SSOe

The IAM SSOe service is an authentication service specifically designed for controlling access for external users accessing VA applications. (For CCRA System Assessing this will be community health providers and their administrators.) This service enhances the user experience by reducing the time associated with multiple logon and logoff activities that require application-specific identifiers and passwords. The service also enables enriched password management and reduction in help desk support.

The SSOe service authenticates users with Cloud Service Provider (CSP) credentials and other externally issued credentials. SSOe retrieves user information from VA authoritative sources to augment the user data provided to integrated applications, and this additional data provides the VA identity context of the user.

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?

All users of CCRA System Assessing are internal to the VA and access is managed via the VA Trusted Internet Connection (TIC) using SSOe or SSOi.

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.

CCRA System Assessing maintains a user role matrix with security groups and role descriptions.

Security Group Name	**Role Description**
VA Facility Community Care Staff – Admin	This is the role of the medical support assistances (MSAs) at the VAMCs. These individuals may work the referral from end to end, including contacting the community providers for appointments, working with the veteran, assigning providers, and working the referral. This group receives most of the auto tasks generated.

Security Group Name	**Role Description**
VA Facility Community Care Staff – Clinical	This role may work the referral from end-to-end. There are certain tasks that go to this group like reviewing medical documentation and reassigning a provider who has been deactivated.
VA Supervisor	This role may work referrals from end-to-end, access the reports menu, and the Manage User Groups menu. This role may also change the referral date and referral expiration date.
VA Read Only	This is a view only role and the user may not change anything on the referral.
VA Reporting Only	This is a view only role however, the user has access to reports.
VA Print Only	This is a view only role with the ability to print the offline referral form.
VA CAR Staff	This role typically only works Claims Adjudication and Reimbursement (CAR), now referred to as Payment Operations and Management (POM) referrals that contain an Emergency or POM SEOC. This role can change the referral date, referral expiration date, and may work a referral without a community provider assigned.
VA CAR Manager	This role is the same as the CAR Staff role with the addition of access to reports.
VA Facility Revenue Manager	This role uses HSRM to receive tasks for precertification reviews and does not modify the referral. This role has access to some reports.
VA Facility Revenue Technician	This role uses HSRM to receive tasks for precertification reviews and does not modify the referral.
VA Insurance Verification Manager	This role uses HSRM to receive tasks for precertification reviews and does not modify the referral. This role has access to some reports.
VA Insurance Verification Staff	This role uses HSRM to receive tasks for reviews and does not modify the referral.
VA RUR Manager	This role for revenue utilization review (RUR) uses HSRM to receive tasks for reviews and does not modify the referral. This role has access to some reports.

Security Group Name	Role Description
VA RUR Nurse	This role for RUR uses HSRM to receive tasks for reviews and does not modify the referral.
CI Admin	This is an executive role at the national level. This role has access to the Manage Optional Task functionality, and it is this role that activates which Optional Tasks may be used for specific VAMCs.
Community Care Provider	This role is assigned to a specific community provider or facility location. The users only see referrals that are assigned to that specific location and specifically to indicate a signature on the electronic Request for Services (RFS) form.
Community Staff	This role is assigned to a specific community provider or facility location. The users only see referrals that are assigned to that specific location.
Community View Only	This role is assigned to a specific community provider or facility location. The users only see referrals that are assigned to that specific location. This is a view only role and the user may not make changes to the referral.
Data Dictionary	This role gives the end user access to the HSRM Data Dictionary.
Community Care Network (CCN) 1	This role may only see referrals that have a CCN1 designation. The user may assign community provider/facility to the referral is there is an optional task assigned to the referral and record appointments.
CCN2	This role may only see referrals that have a CCN2 designation. The user may assign community provider/facility to the referral is there is an optional task assigned to the referral and record appointments.
CCN3	This role may only see referrals that have a CCN3 designation. The user may assign community provider/facility to the referral is there is an optional task assigned to the referral and record appointments.
CCN4	This role may only see referrals that have a CCN4 designation. The user may assign community provider/facility to the referral is there is an optional task assigned to the referral and record appointments.
CCN5	This role may only see referrals that have a CCN5 designation. The user may assign community provider/facility to the

Security Group Name	Role Description
	referral is there is an optional task assigned to the referral and record appointments.
CCN6	This role may only see referrals that have a CCN6 designation. The user may assign community provider/facility to the referral is there is an optional task assigned to the referral and record appointments.
Contractor Admin	This is not an end user role and is for the internal project team and help desk. This role has access to all of the HSRM features.
Wrenches	This is not an end user role and is for internal development use only. On main menu, the user will see a wrench, if user logon has rights to the backend or layout changes.
All Users	All users may add comments, manual tasks, and upload or review documents.
CRM LHS	This user belongs to the auditing groups and may only have access to the task list and is used by Clinical Risk Management (CRM) Lumetra Health Solutions (LHS).
CRM MPRO	This user belongs to the auditing groups and may only have access to the task list and is used by CRM iMPROve (MPRO).
CRM MAX	This user belongs to the auditing groups and may only have access to the task list and is used by CRM Maximus Federal Services (MAX).
CRM PRI	This user belongs to the auditing groups and may only have access to the task list and is used by CRM Provider Resources, Inc. (PRI).

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

Yes, approved VA contractors have access based on their assigned role.

8.2b. What involvement will contractors have with the design and maintenance of the system?

Contractors and subcontractors are subject to confidentiality and nondisclosure agreements from Cognosante and VA. The CCRA System Assessing system is operated and maintained entirely by Cognosante and hosted in the AWS GovCloud environment. System access requires a VA-issued PIV and government-furnished equipment. All contractors require

Talent Management System (TMS) training, annual Privacy and HIPAA-Focused Training (10203), and annual VA Privacy and Information Security Awareness and Rules of Behavior (10176).

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

No

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

No

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

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.

CCRA System Assessing completes new hire and annual Privacy, Security, and HIPAA trainings in both VA TMS and Cognosante's Workday Learning Management System (LMS). These training include, but are not limited to, workforce conduct standards, data handling and protection, social engineering, phishing, malware, and contingency, disaster, and incident response trainings. These trainings are reviewed and updated, at minimum, annually. Both Workday LMS and VA TMS generate email communication when the trainings are due, followed by an acknowledgement once completed.

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

Yes, reference the details in 8.4a.

8.4a If Yes, provide:

1. The Security Plan Status: Approved
2. The System Security Plan Status Date: 06/30/2023

3. The Authorization Status: Approved
4. The Authorization Date: 06/16/2022
5. The Authorization Termination Date: 06/15/2025
6. The Risk Review Completion Date: 02/15/2024
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.***

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, CCRA System Assessing is FedRAMP hosted within AWS GovCloud.

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.*

Not applicable, CCRA System Assessing is FedRAMP hosted within AWS GovCloud.

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.

Not applicable, CCRA System Assessing is FedRAMP hosted within AWS GovCloud.

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.

CCRA System Assessing assigns a senior agency official and lists the privacy laws and regulations in the Contractor Project Management Plan (PMP). These documents are reviewed and signed by CCRA System Assessing Sr. Program Manager, CCRA System Assessing VA IT Program Manager, CCRA System Assessing VA COR, and VA Business Sponsor. These documents establish roles, responsibilities, and access requirements for contractors and service providers and includes privacy requirements in contracts and other acquisition-related documents.

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, CCRA System Assessing is FedRAMP hosted within AWS GovCloud.

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.

ELLER PAMINTUAN

Digitally signed by ELLER PAMINTUAN
Date: 2025.02.07 16:23:50 -07'00'

Privacy Officer, Eller Pamintuan

KIMBERLY KEENE

Digitally signed by KIMBERLY KEENE
Date: 2025.02.11 07:49:31 -05'00'

Information System Security Officer, Kimberly Keene

DENA LISTON

Digitally signed by DENA LISTON
Date: 2025.02.18 17:36:22 -05'00'

Information System Owner, Dena Liston

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).

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
IB 10-163p (va.gov)