Privacy Impact Assessment for the VA IT System called:

Community Care Reimbursement System (CCRS) Assessing

Office of Community Care (HAC)

Date PIA submitted for review:

February 23, 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	julie.drake@va.gov	303.331.7823
Information System Security Officer (ISSO)	Kimberly Keene	Kimberly.Keene@va.gov	703.659.5141
Information System Owner	Brown, Christopher	Christopher.Brown1@va.gov	202-270-1432

Abstract

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

The Community Care Reimbursement System (CCRS) Application is a highly automated system to be used in support of the new Community Care Network (CCN) to align with industry standard invoice reimbursements to fully automate and integrate with other business systems. Required changes are essential to realize the future state Community Care (CC) program model, including a highly integrated and automated system supporting both contracted Community Care Networks and Out of Network invoice processing. The CCRS Application is hosted exclusively as an enterprise deployment system at the VA data center located at Austin Information Technology Center (AITC), Austin, Texas. The CCRS Application is not Veteran facing. CCRS Application is not Internet facing.

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?*
- *Does the system use cloud technology? 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.*
- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*
- *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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

The Application name is Community Care Reimbursement System (CCRS), and the program office that owns the system is Department of Veterans Affairs, Veteran Health Administration, OCC.

The system is to be used to validate claims submitted by contracted entities within the newly established Community Care Network, generate reimbursement payments to the contracted entities, to automate and facilitate post payment audit activities for reimbursements and to automate and facilitate revenue operation activities such as identifying care that requires pre-certification with Other Health Insurance (OHI) agencies, capturing applicable paid claim data and coordination of benefit (COB) information for third party billing and first party copayment liability determination.

The VA Office of Community Care (OCC) requires an automated reimbursement solution, complete with decision-support and robust analytics to enable payment to the Community Care Network (CCN) within seven days. The solution, referred to as the Community Care Reimbursement System (CCRS), will operate as the central repository for CCN claims data and provide data integrity, reimbursement validation, revenue recovery processes, and analytics functionalities that provide meaningful analyses to reduce improper payments. As the CCN grows and operationalizes, CCRS will be configurable and scalable to meet evolving business rules.

VA's mission includes commitments to improving performance, promoting a positive culture of service, increasing operational effectiveness and accountability, advancing healthcare innovation through research, and training future clinicians. VA recognizes that while the healthcare landscape is constantly changing, VA's unique population and broad geographic demands will continue to require community-based care for Veterans. As set forth in 38 Code of Federal Regulation (C.F.R.) 17.1510(b), which may be amended, eligible Veterans may receive healthcare services through the Community Care Network.

The CCRS system is not a Veteran facing system. The CCRS system is not internet facing. User data is not accessible outside of the VA network. Users are not created in the system and users do not have direct access to any data. The CCRS system stores invoice information for medical services provided to Veterans. CCRS stores reference data information that allows the system to run rules for validating the invoice information and making conforming decisions for processing payments. If the system is fully adopted, while the system is not system of record for any medical or financial information, the CCRS system will store transactional data for any Veteran that has received care via the Community Care Network (CCN). There is no 'typical client' impact. If fully adopted, CCRS will serve all eligible Veterans that are registered with VA and that could potentially seek medical care from the Community Care Network Program. There are 22 Million Veterans of the armed forces according to the 2014 US Census Bureau, approximately 10 percent of whom are women, The Veterans Health Administration (VHA) is the largest integrated health care system in the United States, providing care at 1,240 health care facilities, including 180 VA Medical Centers and 1,061 outpatient sites of care of varying complexity (VHA outpatient clinics) to over 9 million Veterans enrolled in the VA. It is estimated that at its highest peak, over 6 million individual data could be processed by CCRS.

CCRS is an application hosted at AITC. CCRS is not deployed to VA sites. There is no CCRS field deployment. CCRS does not communicate or interface with VistA. CCRS does not communicate with any VA hospitals. CCRS is not deployed regionally. CCRS is an enterprise system deployed and operated exclusively from the AITC data center in Austin, VA. CCRS is maintained and operated by EO personnel.

CCRS is an automated payment processing system, which will handle the automation of processing invoices from validation to payment including the verification of payment accuracy of the invoices submitted by the Contracted Community Care Networks (CCNs). The bulk of the system is built using custom Java/J2EE code and ODMiLog/Jrules for conforming and decision support automation and determination of payments and reimbursements of invoices. The System has a SQL server 2016 backend. The System will generate reimbursement payments conforming decisions according to the contract or appropriate rules to the contracted entities, to automate and facilitate post payment audit activities for reimbursements and to automate and

facilitate revenue operation activities such as applicable data from EDI Transmission (837) Coordination of Benefits (COB) information for third party billing and first party copayment liability determination.

It only shares sensitive data internal to the VA network. The connected systems are as follows:
Purchase Care Program Integrity Tool (PIT)
Community Care Referrals and Authorization System (CCRA)
Electronic Data Interchange (EDI) - General
Provider Profile Management System (PPMS)
Central FEE
OM FSC IPPS (Invoice Payment Processing System)
Master Veterans Index (MVI) (formerly known as Master Patient Index (MPI))
VLER Data Access Services (DAS)
IAM Access Services System (IAM AcS)
Palantir

CCRS has only a central set of access controls for operating at AITC. PII is not maintained at any VA sites.

Authority to maintain this system is stated in SORN 114VA16 Program-Billing and Collection Records-VA referencing Title 38, United States Code, sections 1710 and 1729; 23VA10NB3 - Non-VA Care (Fee) Records (Formerly known as 23VA136/23VA16) – VA; 54VA10NB3 - Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA
The completion of this PIA will not result in circumstances that require changes to the business processes.
The completion of this PIA will not result in technology changes.
The system is not modified and will not affect existing SORN, completion of this PIA will not result in SORN changes.
The CCRS is centrally hosted as an enterprise application in AITC server farm. There is no cloud service provider for CCRS.

References:

- FIPS Publication 199; NIST Special Publications 800-30, 800-37, 800-39, 800-60Vol1 and2.
- VA Directive 6508, "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 2014
- VA Handbook 6508, "Procedures for Privacy Threshold Analysis and Privacy Impact Assessment"
- E-government Act of 2002

Section 1. Characterization of the Information

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial Account Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Current Medications
- ☐ Previous Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Other Unique Identifying Number (list below)

Additionally, the following information is collected, processed and retained:
1. Invoice information.
2. Provider Information
3. Claim information (identification, payments, and reimbursements)
4. Eligibility information
5. Date of death
6. Family relationship
7. Eligibility
8. Disability rating
9. Gender
10. Next of Kin
11. Guardian
12. Employment information
13. Veteran dependent information
14. Death certificate information
15. Veteran Service-Connected Status and Conditions)>>

PII Mapping of Components

Community Care Reimbursement System consists of 0 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Community Care Reimbursement System** and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A					

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

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

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The sources of information of the system consist solely, of internal VA systems. The CCRS application is not internet facing or Veteran facing. CCRS collects data from internal system once claims/invoices have been submitted for review and processing. CCRS communicates internally and integrates with other VA systems to gather the information required to make a confirming decision about CCN invoices.

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

CCRS collects Sensitive Personal Information (SPI) to include Personal Identifiable Information (PII) and Protected Health Information (PHI) via secure electronic transfer from VA internal systems as listed in section 4.1

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose. This question is related to privacy control AP-2, Purpose Specification.

CCRS Application is part of the family of systems in CCN program initiative and Major Initiative (MI)-15 Health Care Efficiency. The application interfaces with VA Community Care databases, feeding a repository with an invoice ruling tool that will provide decision support and conforming scoring of incoming invoices for reimbursement to providers in the CC network. The CCRS application will affect the CCN in a positive way by a) reducing the probability of claim backlog and processing and b) ensuring that trust and reimbursement are continually made to CC network providers for medical services already rendered to Veterans.

The information maintained and processed in this CCRS application is not publicly available and not commercial data.

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

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

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

As information for the CCRS Application is imported from existing VA systems, the accuracy is verified by the original source systems prior to transmitting the data to CCRS. CCRS does checks for data type, required fields, null-ability and overall referential compliance to validate the invoices submitted for processing match the authorized and referral episode of care of the Veteran. The CCRS rules engine is a set of custom developed ilog/Jrules based on J2ee code that compare the initial 837 invoice data against reference data provided by CCRS interface partners:
Purchase Care Program Integrity Tool (PIT)
Community Care Referrals and Authorization System (CCRA)
Electronic Data Interchange (EDI) - General
Provider Profile Management System (PPMS)
Central FEE
OM FSC IPPS (Invoice Payment Processing System)

Master Veterans Index (MVI) (formerly known as Master Patient Index (MPI))
VLER Data Access Services (DAS)
IAM Access Services System (IAM AcS)
Palantir

1.6 What specific legal authorities, arrangements, and agreements defined the collection of information?

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

References: FIPS Publication 199; NIST Special Publications 800-30, 800-37, 800-39, 800-60Vol1, 800-60Vol2
(1) 114VA10, The Revenue Program-Billing and Collection Records-VA (Published January 25, 2021)
(2) 23VA10NB3 - Non-VA Care (Fee) Records– VA (Published: 7-30-2015)
(3) 54VA10NB3 - Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (Published: 3-3-2015)
(4) 24VA10A7: Patient Medical Records-VA, (Published: October 2, 2020)
(5) 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) – VA (Published December 23, 2020)
5 U.S.C. § 301 - Departmental Regulations
26 U.S. Code § 61 - Gross Income Defined (a) (12) Income from Discharge of Indebtedness
38 U.S.C. 31 Foreign Medical Program
38 U.S. Code § 109 - Benefits for Discharged Members of Allied Forces
38 U.S. Code § 111 - Payments or Allowances for Beneficiary Travel
38 U.S. Code § 501 - Veterans' Benefits Rules and regulations
38 U.S. Code § 1151 - Benefits for Persons Disabled by Treatment or Vocational Rehabilitation
38 U.S. Code § 1703 - Contracts for Hospital Care and Medical Services in Non-Department Facilities
38 U.S. Code § 1705 - Management of Health Care: Patient Enrollment System
38 U.S. Code § 1710 - Eligibility for Hospital, Nursing Home, and Domiciliary care
38 U.S. Code § 1712 - Dental Care; Drugs and Medicines for Certain Disabled Veterans; Vaccines
38 U.S. Code § 1717 - Home Health Services; Invalid Lifts and Other Devices
38 U.S. Code § 1720 - Transfers for Nursing Home Care; Adult Day Health Care
38 U.S. Code § 1720G - Assistance and Support Services for Caregivers
38 U.S. Code § 1721 - Power to Make Rules and Regulations
38 U.S. Code § 1724 - Hospital Care, Medical Services, and Nursing Home Care Abroad
38 U.S. Code § 1725 - Reimbursement for Emergency Treatment
38 U.S. Code § 1727 -Persons Eligible Under Prior Law
38 U.S. Code § 1728 - Reimbursement of Certain Medical Expenses
38 U.S. Code § 1729 - Recovery by the United States of the cost of certain care and services
38 U.S. Code § 1741-1743. Per Diem Grant- State Home
38 U.S. Code § 1781 - Medical Care for Survivors and Dependents of Certain Veterans
38 U.S. Code § 1786 - Care for Newborn Children of Women Veterans Receiving Maternity Care
38 U.S. Code § 1787 - Health Care of Family Members of Veterans Stationed at Camp Lejeune, NC
38 U.S. Code § 1802-Children of Vietnam Veterans Born with Spina Bifida-Spina bifida conditions

38 U.S. Code § 1803, Sec. 1803 - Children of Vietnam Veterans Born with Spina Bifida -Health care
38 U.S. Code § 1812, 38 U.S. Code 1812 Children of Women Vietnam Veterans Born with Certain Birth Defects, Covered Birth Defects
38 U.S. Code § 1813, 38 U.S. Code 1813 Children of Women Vietnam Veterans Born with Certain Birth Defects- Health Care
38 U.S. Code § 1821 - Benefits for Children of Certain Korea Service Veterans Born with Spina Bifida
38 U.S. Code § 3102 - Basic Entitlement-A Person Shall be Entitled to a Rehabilitation Program
38 U.S. Code § 5701 - Confidential nature of claims
38 U.S. Code § 5724 - Provision of Credit Protection and Other Services
38 U.S. Code § 5727 - Definitions
38 U.S. Code § 7105 - Filing of Notice of Disagreement and Appeal
38 U.S. Code § 7332 - Confidentiality of Certain Medical Records
38 U.S.C. 8131-8137 - Construction Grant- State Home
44 USC – Public Printing Documents
Veterans Access, Choice, and Accountability Act of 2014
38 CFR 2.6 - Secretary's delegations of authority to certain officials (38 U.S.C. 512).
TITLE 45 CFR—Public Welfare Subtitle A—Department of Health and Human Services-Part 60—General Administrative Requirements
45 CFR Part 164 – Security and Privacy
4 CFR 103 – Standards for the Compromise of Claims
Public Law 103–446, section 107 Veterans Education and Benefits Expansion Act of 2001"- Sec. 107. Expansion of Work-Study Opportunities.
Public Law 111–163 section 101. Caregivers and Veterans Omnibus Health Services Act of 2010- Sec. 101. Assistance and Support Services for Caregivers.
Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191.

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

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

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

Follow the format below when entering your risk assessment:

CCRS risk assessment:

Privacy Risk: CCRS collects Personally Identifiable Information (PII) and other Personal Health Information (PHI). If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system and the VA. If the system is breached and data is corrupted the wrong financial reimbursement information could be distributed potentially causing financial loss.

Mitigation: The Department of Veterans Affairs is careful to only collect the minimal information necessary to validate invoices and provide reimbursements for invoices of medical services provided to Veterans By only collecting the minimum necessary information the risk is lowered due to decreased exposure to the data.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

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

CCRS uses the information provided in the 837 COB (invoice, provider and claim information) files to identify a veteran; some of the fields that come in the 837 COB are ICN (including eligibility, date of death, family relationship, disability rating, next of Kin, guardian, employment information, dependent information, death certificate, and service connected status), Veteran's First and Last names, DOB, social security, gender, address, city, state and country where he lives, this information is required to be able to identify a valid veteran. The veteran's names, DOB, gender, and SSN is used to retrieve the ICN from MVI in case the ICN is not present in invoice. We also store medical information that is part of the 837 COB claim lines, this information is used to approved or denied payment. From referrals we get ICN, SSN, First and Last names and DOB, we use this information to validate that the information in the invoice matches the information in the referral.

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

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The ruling and invoice scoring segments of the CCRS application does analyze data to detect and deter conformance of invoices with matched referrals to validate that the invoice processing request matches the episode of care for which the Veteran was authorized. Invoices and decision analysis is made on invoices on a daily basis by comparing daily feeds from VA internal systems. Once all checks are completed the system reports the transactions and decisions, including approval, denials, rejects and holds of invoices for further processing. There is a module in CCRS, the workflow tool, which will support revenue operations audits and post-payment processing of invoices. Invoices flagged for potential audit will be forwarded to the proper authority for manual adjudications and possibly forwarded for further investigations.

No. There are no records placed or updated in the individual VistA record.

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

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

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

Principle of Transparency: 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.

The following SORNs are applicable to the CCRS system:

(1) 114VA10, The Revenue Program-Billing and Collection Records-VA (Published January 25, 2021)
(2) 23VA10NB3 - Non-VA Care (Fee) Records– VA (Published: 7-30-2015)
(3) 54VA10NB3 - Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (Published: 3-3-2015)

(4) 24VA10A7: Patient Medical Records-VA, (Published: October 2, 2020)
(5) 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) – VA (Published December 23, 2020)

SORNs define the information collected from Veterans, use of the information, and how the information is accessed and stored. The information collected is used for determining conformance for payment, reimbursement and validation of invoices for a veteran provided medical services and benefits, such as verification of matching approved and authorized referral feeds with CCN invoices.

There are no external CCRS users in the CCRS application. CCRS System administrators might access the data directly using queries to the database. Access to PII data is limited to system administrator.
Yes. Procedures, controls and roles and responsibilities related to access controls of data are documented.
Yes. Every transaction and access to the system is tracked a logged.
The system administrators are responsible for safeguarding any data stored in CCRS.

The FISMA security controls for the CCRS application cover 17 security areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The RLS application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA HB 6500, VA HB 6500.1, .2, .3, .5, .6,
.8 .11, National Rules of Behavior (ROB), and VA 6502.1, VA 6502.3, VA 6502.4 Privacy Policies govern how veterans' information is used, stored, and protected.

Section 3. Retention of Information

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

3.1 What information is retained?

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

The following information is collected, processed and retained:
1. Invoice information.
2. Provider Information
3. Claim information (identification, payments, and reimbursements)
4. Eligibility information
5. date of death
6. Family relationship
7. Eligibility
8. Disability rating

9. Gender
10. Next of Kin
11. Guardian
12. Employment information
13. Veteran dependent information
14. Death certificate information
15. Veteran Service-Connected Status and Conditions

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

The CCRS System will maintain information related to invoice data, (for 6 years) and referral and authorization and provider profile data for as long as the system is operational as an enterprise supporting system to the CCN.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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

VHA Record Control Schedule (RCS) 10–1
https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf
Yes, 1260 Civilian Health and Medical Care Program Page II-1-55 Electronic Records (Master Files). Electronic records produced form scanned documents or records received electronically (optical disk, magnetic tape or other electronic medium).
Temporary; destroy 6 years after all individuals in the record become ineligible for program benefits. (N1-15-03-1,
item 3)

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.?
This question is related to privacy control DM-2, Data Retention and Disposal

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA 6500.1 HB Electronic Media Sanitization, Per the Veterans Health Administration Records Control Schedule: RCS 10-1.
Disposition of Printed Data: Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks and disposed of properly (when the approved records schedule permits destruction) by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers. Output document. Paper copies of documents generated form electronic files. Temporary; destroy when no longer needed. (N1-15-03-1, item 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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

CCRS does ***not use*** any PII or Veteran data for any purposes other than the intended ruling and decision support of conforming invoices and ruling. CCRS policies and procedures been developed to neutralize, avoid, prohibit and minimize the use of PII for testing, training, and research.

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

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

<u>Principle of Minimization:</u> Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

<u>Principle of Data Quality and Integrity:</u> Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

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

Mitigation: To mitigate the risk posed by information retention, the CCRS Application adheres to the VA RCS schedules for each category or data it maintains.

When the retention data is reached for a record, the AITC EO will carefully dispose of the data by the determined method as described in question 3.4. VA Handbook 6500.2, Management of Data Breaches Involving Sensitive Personal Information (SPI), which contains the policies and responsibilities that VA components are required to follow to manage data breaches, including detection, correlation, notification, remediation, and reporting. CCRS follows the VA RCS 10-1 and timely purges data.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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

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.

This is a VA self-contained system hosted at AITC. It only shares sensitive data internal to the VA network. The CCRS connected systems are as follows:
The connected systems are as follows:
Purchase Care Program Integrity Tool (PIT)
Community Care Referrals and Authorization System (CCRA)

Electronic Data Interchange (EDI) - General
Provider Profile Management System (PPMS)
Central FEE
OM FSC IPPS (Invoice Payment Processing System)
Master Veterans Index (MVI) (formerly known as Master Patient Index (MPI))
VLER Data Access Services (DAS)
IAM Access Services System (IAM AcS)
Palantir

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Purchase Care Program Integrity Tool (PIT)	CCRS send data to PIT for audit, fraud, waste and abuse investigation	CCRS sends the Individual Control Number (ICN); Social Security Number (SSN); Date of Birth (DOB); First Name; Last Name; Gender; Medical Procedure Information. This information is sent to PIT for fraud detection processing	Secure data transfer via Windows file share using a Drop zone behind the VA firewall, integration of data into PIT.
Community Care Referrals and Authorization System (CCRA)	CCRA sends data from CCRS related to the authorized and referred episode of care for Veterans	CCRA sends to CCRS the referral; patient information, SSN, ICN, DOB, First Name; Last Name; Gender; Pre-Authorization information CCRS receives this information so it can validate the invoice information against the information in the referral	Secure data transfer via file share using a drop zone behind the VA firewall.
Electronic Data Interchange (EDI) - General	EDI sends to CCRS the data related to invoices for processing and reimbursements	EDI sends to CCRS the data related to invoices for processing and reimbursements CCRS will receive. As part of the invoice,	Secure data transfer via Windows file share using a drop zone behind the VA firewall, with subsequent, secure Extract Transform Load (ETL)

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
		PII information that will be used to approve or deny payments.	Integration of data into CCRS.
Provider Profile Management System (PPMS)	PPMS sends data to CCRS related to the provider for validation of provider information contained in the 837 invoices	CCRS sends the National Provider Identifier; Community Care Network Identification; Date of Service. With this information, PPMS will validate if the provider is active and not in the LEIE list and reply with a Yes or No answer	Secure data transfer via OData service data share using a service zone behind the VA firewalls.
Central FEE	CCRS sends data to Central Fee processed and paid invoice information for annual budget reconciliations	CCRS sends data to Central Fee Veteran ICN; First Name; Middle Name; Last Name; DOB. This information is going to be used by Central Fee to Identify a veteran	Secure data transfer via Windows file share using a drop zone behind the VA firewall, with subsequent, secure Extract Transform Load (ETL) Integration of data into CCRS.
OM FSC IPPS (Invoice Payment Processing System)	CCRS sends electronic invoice data and IPPS provides approval/acceptance workflow and FMS payment transaction creation	CCRS sends instructions for payment to IPPS and gets back payment confirmation	The transmission to CDW might happen thru PIT and not directly from CCRS, this still needs to be defined.
Master Veterans Index (MVI) (formerly known as Master Patient Index (MPI))	MVI sends Veteran data to CCRS to validate Veterans records present in the 837 invoices	CCRS sends to MVI the SSN; First Name; Last Name; Middle Initial (if provided); DOB; Gender. This information is used by MVI to identify a veteran and then return the ICN to CCRS, after receiving the ICN, CCRS stores it as part	Secure data transfer via MVI service data share using a service zone behind the VA firewall

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
		of the patient information.	
VLER Data Access Services (DAS)	DAS sends data to CCRS related to the per member, per month administrative fees	DAS sends data to CCRS the PMPM report that will be used by CCRS to verify service fee charges, CCRS sends back the PMPM report with all processed records and any error codes. CCRS also submits to DAS the Reconciliation report that will be used by the CCNs to verify payments processing and any type of rejection or deny of payment. The fields submitted to with the reconciliation report are: • Referral Number • Date of Service • Provider NPI	Secure data transfer via Windows file share using a drop zone behind the VA firewall, with subsequent, secure Extract Transform Load (ETL) Integration of data into CCRS.
IAM Access Services System (IAM AcS)	IAM provides secured accounts to CCRS so that applications can share data in the VA enterprise in accordance to VA6500	CCRS sends to MVI a request for authentication so the MVI service can be accessed, IAM returns an authorization token that is used to talk to MVI	Secured accounts provided by IAM integration services.
Palantir	Palantir is a data analytics and integration tool that allows authorized users to upload, manage, and track data and actions taken on that data. We currently foresee doing	Patient-level health record information, Hospital capacity data, supply chain data for critical medical supplies and medical equipment, Diagnostic testing data, CDC COVID-19	HTTPS over 443, JDBC

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
	analytics related to supply chain, waste fraud and abuse, and purchase/contract data. This product is used by VA staff, primarily business and financial analyst personnel, as well as executive leadership for visibility of Enterprise Business Intelligence data. This is a SaaS hosted in AWS.	tracking data, Veterans population data, and VA health care enrollee data	

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: The CCRS privacy risk associated with maintaining PII is that sharing data within the Department of Veterans' Affairs could happen and that the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by CCRS personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within. Access control is accomplished through the use of MyVA ePAS, secured tokens, secured accounts, VA form 9957 with the end user's manager approval and authorized by the appropriate System Manager of Record (SMR) or System Manager of Record Designee (SMRD).

Section 5. External Sharing/Receiving and Disclosure

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

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

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

Note: This question is #7 in the Privacy Threshold Analysis.

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

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

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

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

Data Shared with External Organizations

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

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

In order to protect CCRS veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:

1. The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.
4. Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls.

Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: There is a risk that information may be shared with an unauthorized program, system, or individual.

Mitigation: The System Interconnection Agreement/Memorandum of Understanding is in place with CCRS partners, including CCRA and PPMS. These documents define the terms and conditions for sharing the data internal to the VA. Safeguards are implemented to ensure data is not sent to the wrong organization, program or system. VA employees, contractors and business partners take security and privacy training and awareness and are required to report suspicious activity. Use of secure passwords, access for need to know basis, encryption, and access authorization are all measures that are utilized within the facilities.

Section 6. Notice

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

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

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

The Department of Veterans Affairs does provide public notice that the CCRS system does exist. Please note that CCRS is not Veteran facing or internet facing. This notice is provided in various ways:

1. Systems of Record Notices outline the collection and use of information in each of these SORNS: https://www.oprm.va.gov/docs/Current_SORN_List_02_02_2021.pdf

(1) 114VA10, The Revenue Program-Billing and Collection Records-VA (Published January 25, 2021)
(2) 23VA10NB3 - Non-VA Care (Fee) Records– VA (Published: 7-30-2015)
(3) 54VA10NB3 - Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (Published: 3-3-2015)
(4) 24VA10A7: Patient Medical Records-VA, (Published: October 2, 2020)
(5) 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) – VA (Published December 23, 2020)

2. This Privacy Impact Assessment (PIA) also serves as notice of CCRS. 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." Additionally, Individuals may receive Privacy Notice at the time they have their data captured by the source systems supplying data to CCRS.

3. For VHA related Privacy Notification online can be found at: http://www.va.gov/health/ after getting to the website select VA Privacy Practices link (as shown below) on the lower right side of the web page.

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

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached.
This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress

No opportunity or right to decline to provide information is provided by CCRS. No information is collected from the veteran by CCRS.

Any opportunity or notice of the right to decline to provide information given to the veteran would be given at the point of service. A copy of the Privacy Notice is provided in appendix A.

CCRS is not Veteran facing. CCRS is not internet facing.

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

Any right to consent to particular uses of the information would be handled by the source systems (PPMS. MVI, CCR&A, DAS) that collect the information from the veteran and feed CCRS with information. CCRS is not Veteran facing. CCRS is not internet facing.

6.4 PRIVACY IMPACT ASSESSMENT: Notice
Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

Follow the format below:

Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by CCRS

Mitigation: The VA mitigates this risk by providing the public with notice provided at the time of authorization and referrals at the VA Medical Center also by following the guidelines of SORNS as shown in above section 6.1.

Section 7. Access, Redress, and Correction

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

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

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

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

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

CCRS is not Veteran facing and is not internet facing. CCRS is an internal system only accessible to VA employees. individuals are not able to access their information directly through CCRS. Individuals wishing to obtain more information about access, redress and record correction of CCRS data should contact the Department of Veteran's Affairs as directed in the System of Record Notices

(1) 114VA10, The Revenue Program-Billing and Collection Records-VA (Published January 25, 2021)
(2) 23VA10NB3 - Non-VA Care (Fee) Records– VA (Published: 7-30-2015)
(3) 54VA10NB3 - Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (Published: 3-3-2015)
(4) 24VA10A7: Patient Medical Records-VA, (Published: October 2, 2020)
(5) 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) – VA (Published December 23, 2020)

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 wishing to obtain more information about access, redress and record correction of CCRS data should contact the Department of Veteran's Affairs regional as directed in the System of Record Notices:
(1) 114VA10, The Revenue Program-Billing and Collection Records-VA (Published January 25, 2021)
(2) 23VA10NB3 - Non-VA Care (Fee) Records– VA (Published: 7-30-2015)
(3) 54VA10NB3 - Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (Published: 3-3-2015)
(4) 24VA10A7: Patient Medical Records-VA, (Published: October 2, 2020)
(5) 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) – VA (Published December 23, 2020)

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 wishing to obtain more information about access, redress and record correction of CCRS data should contact the Department of Veteran's Affairs regional as directed in the System of Record Notices; Individuals are notified by the following SORNs:
(1) 114VA10, The Revenue Program-Billing and Collection Records-VA (Published January 25, 2021)
(2) 23VA10NB3 - Non-VA Care (Fee) Records– VA (Published: 7-30-2015)
(3) 54VA10NB3 - Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (Published: 3-3-2015)
(4) 24VA10A7: Patient Medical Records-VA, (Published: October 2, 2020)
(5) 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) – VA (Published December 23, 2020)

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Beneficiary Programs: Individuals may contact the Customer Service telephone line at 1-800-733-8387
Veterans Programs: Individuals may contact the Customer Service telephone line at 1-877-881-7618

Individuals cannot access CCRS directly and can follow the steps listed in 7.2 or use the numbers provided above for redress.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that individuals may seek to access or redress records about them held by the CCRS system and may not know the procedure to accomplish the task. >>

Mitigation: Individuals wishing to obtain more information about access, redress and record correction of CCRS data should contact the Department of Veteran's Affairs regional as directed in the System of Record Notices:

(1) 114VA10, The Revenue Program-Billing and Collection Records-VA (Published January 25, 2021)
(2) 23VA10NB3 - Non-VA Care (Fee) Records– VA (Published: 7-30-2015)
(3) 54VA10NB3 - Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (Published: 3-3-2015)
(4) 24VA10A7: Patient Medical Records-VA, (Published: October 2, 2020)
(5) 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) – VA (Published December 23, 2020)

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

-Describe the process by which an individual receives access to the system.
Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?
-Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls. The supervisor/COR documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring is performed through the use of VA's Talent Management System (TMS). MyVA ePAS and VA form 9957 are used when creating accounts and granting appropriate access. Account access will be managed through the internal 9957 process which authorizes users of the information system and specifying access privileges. CCRS uses Active Directory (AD) Service Desk Management (SDM) to determine access to metadata within the application.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.
This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Contractors working on CCRS, usually referred as 'contracted employees', from other external government agencies will not have access to CCRS. Contractors will not be accessing any CCRS information. There is no requirement for signatures on NDAs, or confidentiality agreements. Contractor access is verified through VA personnel before access is granted to any contractor. Contracts and contractor access are reviewed annually at a minimum. The contractors who provide support to the system are required to complete annually and before access in TMS:
VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176)
Privacy and HIPAA Training (VA 10203)
All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access.

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.

Personnel who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Information Security Rules of Behavior (RoB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's TMS. After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. This training includes, but is not limited to, the following TMS Courses:

- VA 10176: Privacy and Info Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training
- VA 3812493: Annual Government Ethics

Role-based Training
Includes, but is not limited to and based on the role of the user.
VA 1016925: Information Assurance for Software Developers IT Software Developers
VA 3193: Information Security for CIOs Executives, Senior Managers, CIOs and CFOs
VA 1357084: Information Security Role-Based Training for Data Managers
VA 64899: Information Security Role-Based Training for IT Project Managers
VA 3197: Information Security Role-Based Training for IT Specialists
VA 1357083: Information Security Role-Based Training for Network Administrators
VA 1357076: Information Security Role-Based Training for System Administrators
VA 3867207: Information Security Role-Based Training for System Owners

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

1. *The date the Authority to Operate (ATO) was granted,*
   Granted on 27 Sep 2020
2. *Whether it was a full ATO or ATO with Conditions,*
   Full ATO
3. *The amount of time the ATO was granted for,*
   Full ATO granted for 3 years
4. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH)*
   System Classified as - Moderate

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

If No or In Process, provide your ***Initial Operating Capability (IOC) date.***
IOC date: 09 April 2020

CCRS (CCN) is currently progressing through the Risk Management Framework Process for review and authority to operate approval.

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

JULIE C. DRAKE 969177

Digitally signed by JULIE C. DRAKE 969177
Date: 2021.03.04 10:30:41 -07'00'

Privacy Officer, Julie Drake

Kimberly D. Keene 106407

Digitally signed by Kimberly D. Keene 106407
Date: 2021.03.04 12:17:10 -05'00'

Information Security Systems Officer, Kimberly Keene

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2021.03.03 16:09:20 -06'00'

System Owner, Brown, Christopher

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).