Privacy Impact Assessment for the VA IT System called:

Community Care Reimbursement System– (VAEC–AWS)

Office of Integrated Veteran Care
Veterans Health Administration

Date PIA submitted for review:

09/20/2022

System Contacts:

System Contacts

	Name	E–mail	Phone Number
Privacy Officer	Michael Hartmann	Michael.Hartmann@va.gov	303.780.4753
Information System Security Officer (ISSO)	Amine Messaoudi	Amine.Messaoudi@va.gov	202.815.9345
Information System Owner (ISO)	Christopher Brown	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 (VAEC–AWS) application is a highly automated system used to validate invoices submitted by contracted entities within the Integrated Veteran Care Network (IVC). The primary objective is 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 of the 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 CC–CCRS–VAEC–AWS Application is not Internet facing. The CC–CCRS–VAEC–AWS Application is not accessible to Veterans.

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The name of the IT system is Community Care Reimbursement System Veteran Affairs Enterprise Cloud Amazon Web Service (CC–CCRS–VAEC–AWS) and the Program Office that owns the system is Department of Veterans Affairs (VA), Veteran Health Administration (VHA), Office of Integrated Veteran Care (IVC). CCRS is currently hosted at VAEC–AWS Cloud.

IVC 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 CC–CCRS–VAEC–AWS, operates as the central repository for CCN claims data and provides data integrity, reimbursement validation, revenue recovery processes and analytics functionalities that provide meaningful analyses to reduce improper payments. As the CCN grows and operationalizes, CC–CCRS–VAEC–AWS will be configurable and scalable to meet evolving business rules.

The CC–CCRS–VAEC–AWS system is used to validate claims submitted by contracted entities within the established CCN. The system validates reimbursement payments, automates and facilitates post payment audit activities for reimbursements and automates revenue operation activities. These activities identify 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 CC–CCRS–VAEC–AWS Application is not accessible to Veterans. The CC–CCRS–VAEC–AWS 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 CC–CCRS– VAEC–AWS system stores invoice information for medical services provided to Veterans. CC– CCRS–VAEC–AWS stores reference data information that allows the system to run rules for validating the invoice information and making conforming decisions for processing payments. There is no 'typical client' impact. CC–CCRS–VAEC–AWS serves all eligible Veterans that are registered with VA that could potentially seek medical care from the Community Care Network Program. According to the 2014 US Census Bureau, there are 22 million Veterans of the armed forces of which approximately 10 percent are women. The Veterans Health Administration (VHA) is the largest integrated health care system in the United States. The VHA provides 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 individuals' data could be processed by CC–CCRS–VAEC–AWS.

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.

CC–CCRS–VAEC–AWS is Amazon Web Service for VA Cloud services based and is not deployed to VA sites and there is no field or regional deployment. CC–CCRS–VAEC–AWS does not communicate or interface with Veterans Health Information Systems and Technology Architecture (VistA) nor does it communicate with any VA hospitals.

CC–CCRS–VAEC–AWS 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 Operational Decision Manager (ODM) iLog/Jrules for conforming and decision support automation and determination of payments and reimbursements of invoices. The System has a Microsoft SQL server v2016 backend. The System

will generate reimbursement payment 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 Electronic Data Interchange (EDI) Transmission (837) Coordination of Benefits (COB) information for third–party billing and first–party copayment liability determination.

CC–CCRS–VAEC–AWS only shares sensitive data internal to the VA network. The connected systems are as follows:

- Program Integrity Tool (PIT)
- Community Care Referrals and Authorization System Assessing (CCRA)
- Electronic Data Interchange (EDI) – General
- Provider Profile Management System (PPMS) Assessing
- Financial Management System (FMS)
- Identity and Access Management System (IAM)
- Data Access Services (DAS Cloud) Assessing
- Master Patient Index (MPI)

Authority to maintain this system is stated in SORNs:

- 23VA10NB3, Non–VA Care (Fee) Records – VA (7/30/2015)
- 24VA10A7, Patient Medical Records – VA (10/2/2020)
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (3/3/2015)
- 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA (12/23/2020)
- 114VA10, The Revenue Program–Billing and Collection Records – VA (1/25/2021)

Section 1. Characterization of the Information

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

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

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

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

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

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

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

1. Claim information (identification, payments, and reimbursements)
2. Date of death
3. Family relationship
4. Disability rating
5. Guardian
6. Employment information
7. Veteran dependent information
8. Death certificate information
9. Medical Records
10. Zip Code

PII Mapping of Components

Community Care Reimbursement System (VAEC–AWS) consists of one key component(s): (databases). 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 (VAEC–AWS) and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
CCRS SQL Server Database provided as a service that is hosted by VAEC	No	Yes	Name, Integration Control Number, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers, Medical records, Claim Information, Race/Ethnicity, Date of Death, Family Relationship, Disability Rating, Gender, Next of Kin, Guardian, Employment Information, Veteran Dependent Information, Death Certificate Information	Claims Processing	Secure File Transfer Protocol (SFTP) over secured encryption and leveraging Identity Access Management (IAM) security accounts.

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 consist solely of internal VA systems listed in paragraph 4.1. The CC–CCRS–VAEC–AWS application is not internet facing. The CC–CCRS–VAEC–AWS application is not accessible to Veterans. CC–CCRS–VAEC–AWS collects data from internal systems once claims/invoices have been submitted for review and processing. CC–CCRS–VAEC–AWS 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.

CC–CCRS–VAEC–AWS 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 1.5.

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

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is

there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

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

CC–CCRS–VAEC–AWS Application is part of the family of systems in the Community Care Network (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 CCN. The CC–CCRS–VAEC–AWS application will:

a) reduce the probability of claim backlog and processing and;
b) ensure that trust and reimbursement are continually made to CCN providers for medical services already rendered to Veterans.

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

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

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

References: FIPS Publication 199; NIST Special Publications 800–30, 800–37, 800–39, 800–60Vol1, 800–60Vol2
(1) 23VA10NB3, Non–VA Care (Fee) Records – VA (7/30/2015)
(2) 24VA10A7, Patient Medical Records – VA (10/2/2020)
(3) 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (3/3/2015)
(4) 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA (12/23/2020)
(5) 114VA10, The Revenue Program–Billing and Collection Records – VA (1/25/2021)
5 U.S. Code § 301 – Departmental Regulations
26 U.S. Code § 61 – Gross Income Defined (a) (12) Distributive share of partnership gross income

38 U.S. Code § 31 – Training and Rehabilitation for Veterans with Service–Connected Disabilities
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 – Veterans Community Care Program
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 – Criteria for Payment – Applications
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, North Carolina
38 U.S. Code § 1802 Spina Bifida Conditions Covered
38 U.S. Code § 1803, Sec. 1803 – Children of Vietnam Veterans Born with Spina Bifida – Health Care
38 U.S. Code § 1812 – Covered Birth Defects
38 U.S. Code § 1813 – Children of Women Vietnam Veterans Born with Certain Birth Defects
38 U.S. Code § 1821 – Benefits for Children of Certain Korea Service Veterans Born with Spina Bifida
38 U.S. Code § 3102 – Basic Entitlement – Training and Rehabilitation for Veterans with Service–Connected Disabilities
38 U.S. Code § 5701 (b)(6)(g)(2)(g)(4)(c)(1) – Confidential nature of claims
38 U.S. Code § 5724 – Provision of Credit Protection and Other Services
38 U.S. Code § 7105 – Filing of Appeal
38 U.S. Code § 7301(a) – Functions of Veterans Health Administration: in general
38 U.S. Code § 7332 – Confidentiality of Certain Medical Records
38 U.S. Code § 8131–8137 – Veterans Benefits– State Control of Operations
44 U.S. Code – Public Printing and 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)
45 CFR – Public Welfare Subtitle A – Department of Health and Human Services
45 CFR Part 160 – General Administrative Requirements
45 CFR Part 164 – Security and Privacy
4 CFR Part 103 – Standards for the Compromise of Claims
Public Law 103 – 446, Section 107. Evaluation of health status of spouses and children of

Persian Gulf War veterans
Public Law 111 – 163 Section 101. Assistance and Support Services for Caregivers
Public Law 104 – 191. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Privacy Risk: CC–CCRS–VAEC–AWS collects Personally Identifiable Information (PII) and other Personal Health Information (PHI). If this information was breached, accidentally released to inappropriate parties or the public and/or inaccurate data is received 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 CC–CCRS–VAEC–AWS is an internal system that uses data provided to the database through the appropriate agencies; therefore, lowering the risk by reducing access to only approved individuals. The Department of Veterans Affairs (VA) collects invoices and decision(s) analysis that are made daily 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.

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.

CC–CCRS–VAEC–AWS uses the information provided in the 837 Coordination of Benefit (COB) invoice (provider and claim information files) to identify a veteran. Some of the fields that come in the 837 COB are the Integration Control Number (ICN), 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, Date of Birth (DOB), social security number (SSN), gender and the address, city, state and country where the Veteran lives. This information is required in order to be able to identify a valid veteran. The Veteran's names, DOB, gender, and SSN are used to retrieve the ICN from Identity and Access Management (IAM) Assessing in case the ICN is not present on the invoice. We also store medical information that is part of the 837 COB claim lines. This information is used to approve or deny payment.

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 CC–CCRS–VAEC–AWS application does analyze data to detect and deter conformance of invoices with matched referrals to validate the invoice processing request matches the episode of care for which the Veteran was authorized. Invoices and decision analysis are made on invoices daily 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 CC–CCRS– VAEC–AWS, 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.

2.3 How is the information in the system secured?

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

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

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

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

CC–CCRS–VAEC–AWS System administrators might access the data directly using queries to the SQL database provided as a service that is hosted within VAEC. Access to PII data is limited to the system administrator. Procedures, controls, and roles and responsibilities related to access controls of data are documented. Every transaction and access to the system is tracked and logged on the SQL database. All CC–CCRS–VAEC–AWS personnel are required to complete VA Privacy and Information Security Awareness and Rules of Behavior Training and Privacy and HIPAA Training annually and appropriate role–based training before access to the system is granted. The system administrators are responsible for safeguarding any data stored in CC–CCRS–VAEC–AWS.

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

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

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

Principle of Transparency: 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.

CC–CCRS–VAEC–AWS System administrators might access the data directly using queries to the SQL database provided as a service that is hosted within VAEC. Access to PII data is limited to the system administrator. Procedures, controls, and roles and responsibilities related to access controls of data are documented. Every transaction and access to the system is tracked and logged on the SQL database. All CC–CCRS–VAEC–AWS personnel are required to complete VA Privacy and Information Security Awareness and Rules of Behavior Training and Privacy and HIPAA Training annually and appropriate role–based training before access to the system is granted. The system administrators are responsible for safeguarding any data stored in CC–CCRS–VAEC–AWS. System owner(s) approval is required for those requesting access to the system.

Section 3. Retention of Information

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

3.1 What information is retained?

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

The following information is collected, processed, and retained:
Name
1. Social Security Number
2. Date of Birth
3. Address
4. Health Insurance Beneficiary Numbers
5. Race / Ethnicity
6. Integration Control Number
7. Claim information (identification, payments, and reimbursements)
8. Date of death
9. Family relationship
10. Disability rating
11. Gender
12. Next of Kin
13. Guardian
14. Employment information
15. Veteran dependent information
16. Death certificate information
17. Medical Records
18. Zip Code

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM–2, Data Retention and Disposal.

The CC–CCRS–VAEC–AWS system retains funding records on paid claims for six years and a monthly schedule will be created for disposal of those records.

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: vaww.va.gov/vhapublications/rcs10/rcs10–1.pdf

Yes, the retention schedule has been approved by the VA Records Office and the National Archives and Records Administration (NARA).
1260 Civilian Health and Medical Care Program Page II–1–55 Electronic Records (Master Files).
Electronic records produced from 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, as applicable (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 OIT–OIS SOP 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, Destruction of Temporary Paper Records. 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 paper documents formed by electronic files are stored in the appropriate repositories. Temporary– destroy when no longer needed as applicable (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

CC–CCRS–VAEC–AWS uses techniques such as fictious names and other false PII related information during research, testing, and/or training. CC–CCRS–VAEC–AWS does not use any PII or Veteran data for any purposes other than the intended ruling and decision support of conforming invoices and ruling. CC–CCRS–VAEC–AWS policies and procedures have 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:

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

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

Privacy Risk: There is a risk that the information maintained by CC–CCRS–VAEC–AWS 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 CC–CCRS–VAEC–AWS Application adheres to the VA RCS schedules for each category or data it maintains. If the retention data is breached for a record, procedures from VA Handbook 6500.2 will be followed. VA Handbook 6500.2, Management of Data Breaches Involving Sensitive Personal Information (SPI) contains the policies and responsibilities that VA components are required to follow to manage data breaches, including detection, correlation, notification, remediation, and reporting.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Health Administration (VHA), Program Integrity Tool (PIT)	Validate claims using a scoring tool that scores incoming claims for risk of fraud, waste, and abuse.	Name, Integration Control Number, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers, Medical records, Claim Information, Race/Ethnicity, Date of Death, Family Relationship, Disability Rating, Gender, Next of Kin, Guardian, Employment Information, Veteran Dependent Information, Death Certificate Information	Drop zone, file transmission using Secure File Transfer Protocol (SFTP) over secured encryption and leveraging Identity Access Management (IAM) security accounts. Network connection over port 443 orchestrated by a Kafka service.
Veterans Health Administration (VHA), Electronic Data Interchange (EDI) – General	Directory of authorized providers within the VA Network	Name, Integration Control Number, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers, Medical records, Claim Information, Race/Ethnicity, Date of	Drop zone, file transmission using SFTP over secured encryption and leveraging IAM security accounts. PPMS

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		Death, Family Relationship, Disability Rating, Gender, Next of Kin, Guardian, Employment Information, Veteran Dependent Information, Death Certificate Information	is hosted in VAEC Visionary Artistry Magazine (VAMAG). Network connection over port 443 orchestrated by a Kafka service
Veterans Health Administration (VHA), Financial Management System (FMS)	Funding measurements and authorizations	Name, Integration Control Number, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers, Medical records, Claim Information, Race/Ethnicity, Date of Death, Family Relationship, Disability Rating, Gender, Next of Kin, Guardian, Employment Information, Veteran Dependent Information, Death Certificate Information	Drop zone, file transmission using SFTP over secured encryption and leveraging IAM security accounts. Network connection over port 443 orchestrated by a Kafka Service
Veterans Health Administration (VHA), Identity and Access Management Assessing (IAM)	Transport of the Veterans health, benefits, or administrative data between consumers and producers	Name, Integration Control Number, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers, Medical records, Claim Information, Race/Ethnicity, Date of Death, Family Relationship, Disability Rating, Gender, Next of Kin, Guardian, Employment Information, Veteran Dependent Information, Death	Drop zone, file transmission using SFTP over secured encryption and leveraging IAM security accounts. Network connection over port 443 orchestrated by a Kafka service

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		Certificate Information	
Veterans Health Administration (VHA), Community Care Referrals and Authorization System Assessing (CCRA)	Validate claim status for Treasury and Financial Management System	Name, Integration Control Number, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers, Medical records, Claim Information, Race/Ethnicity, Date of Death, Family Relationship, Disability Rating, Gender, Next of Kin, Guardian, Employment Information, Veteran Dependent Information, Death Certificate Information	Drop zone, file transmission using Secure File Transfer Protocol (SFTP) over secured encryption and leveraging Identity Access Management (IAM) security accounts. Network connection over port 443 orchestrated by a Kafka service.
Veterans Health Administration (VHA), Provider Profile Management System (PPMS) Assessing	Directory of authorized providers within the VA Network	Name, Integration Control Number, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers, Medical records, Claim Information, Race/Ethnicity, Date of Death, Family Relationship, Disability Rating, Gender, Next of Kin, Guardian, Employment Information, Veteran Dependent Information, Death Certificate Information	Drop zone, file transmission using SFTP over secured encryption and leveraging IAM security accounts. PPMS is hosted in VAEC Visionary Artistry Magazine (VAMAG). Network connection over port 443 orchestrated by a Kafka service
Veterans Health Administration (VHA), Master Patient Index (MPI)	The SSN is required for transmittal of data to downstream applications (PIT, ROWT)	ICN, SSN, Date of Birth, Sex, Address, City, State Code, Postal Code, Country Code, First Name, Middle Name, Last Name	Verification and retrieval of veteran's data elements to perform business rules validation. XML payload via HTTPS, secured by a two–way

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
			exchange of SSL certificates.
Veterans Health Administration (VHA), Data Access Services (DAS Cloud) Assessing	Transport of the Veterans health, benefits, or administrative data between consumers and producers	Name, Integration Control Number, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers, Medical records, Claim Information, Race/Ethnicity, Date of Death, Family Relationship, Disability Rating, Gender, Next of Kin, Guardian, Employment Information, Veteran Dependent Information, Death Certificate Information	Drop zone, file transmission using SFTP over secured encryption and leveraging IAM security accounts. Network connection over port 443 orchestrated by a Kafka service

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.

Privacy Risk: The CC–CCRS–VAEC–AWS 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 CC–CCRS–VAEC–AWS 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 Electronic 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: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
None	None	None	None	None

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

Privacy Risk: NA. There is no external sharing.

Mitigation: NA. There is no external sharing.

Section 6. Notice

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

6.1 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.

1. Systems of Record Notices outline the collection and use of information in each of these SORNS:

- 23VA10NB3, Non–VA Care (Fee) Records – VA (7/30/2015)
- 24VA10A7, Patient Medical Records – VA (10/2/2020)
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (3/3/2015)
- 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA (12/23/2020)
- 114VA10, The Revenue Program–Billing and Collection Records – VA (1/25/2021)

2. This Privacy Impact Assessment (PIA) also serves as notice of CC–CCRS–VAEC–AWS. 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 a Privacy Notice at the time they have their data captured by the source systems supplying data to CC–CCRS–VAEC–AWS.

3. VHA related Privacy Notification online can be found at: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090.

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

The CC–CCRS–VAEC–AWS Application is not accessible to Veterans. CC–CCRS–VAEC–AWS is not internet facing. CC–CCRS–VAEC–AWS receives data from other VA Systems; therefore, the individual must contact the primary system that maintains the data.

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 uses of the information would be handled by the source systems (PIT, CCRA, EDI, PPMS, FMS, IAM, MPI and DAS Cloud) that collect the information from the veteran and feed CC–CCRS–VAEC–AWS with information.
The CC–CCRS–VAEC–AWS Application is not accessible to Veterans. CC–CCRS–VAEC–AWS 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

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

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.

CC–CCRS–VAEC–AWS is not internet facing. The CC–CCRS–VAEC–AWS Application is not accessible to Veterans. CC–CCRS–VAEC–AWS is an internal system only accessible to VA employees. Individuals are not able to access their information directly through CC–CCRS–VAEC– AWS. Individuals wishing to obtain more information about access, redress and record correction of CC–CCRS–VAEC–AWS data should contact the Department of Veteran's Affairs as directed in SORNs:

- 23VA10NB3, Non–VA Care (Fee) Records – VA (7/30/2015)
- 24VA10A7, Patient Medical Records – VA (10/2/2020)
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (3/3/2015)
- 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA (12/23/2020)
- 114VA10, The Revenue Program–Billing and Collection Records – VA (1/25/2021)

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 CC– CCRS–VAEC–AWS data should contact the Department of Veteran's Affairs regional as directed in SORNs:

- 23VA10NB3, Non–VA Care (Fee) Records – VA (7/30/2015)
- 24VA10A7, Patient Medical Records – VA (10/2/2020)
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (3/3/2015)
- 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA (12/23/2020)
- 114VA10, The Revenue Program–Billing and Collection Records – VA (1/25/2021)

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 CC– CCRS–VAEC–AWS data should contact the Department of Veteran's Affairs regional as directed in the System of Record Notices; Individuals can obtain information by accessing the following SORNs:

- 23VA10NB3, Non–VA Care (Fee) Records – VA (7/30/2015)
- 24VA10A7, Patient Medical Records – VA (10/2/2020)
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (3/3/2015)
- 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA (12/23/2020)
- 114VA10, The Revenue Program–Billing and Collection Records – VA (1/25/2021)

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 CC–CCRS–VAEC–AWS 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.

Privacy Risk: There is a risk that individuals may seek to access or redress records about them held by the CC–CCRS–VAEC–AWS 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 CC–CCRS–VAEC–AWS data should contact the Department of Veteran's Affairs regional as directed in SORNs:

- 23VA10NB3, Non–VA Care (Fee) Records – VA (7/30/2015)
- 24VA10A7, Patient Medical Records – VA (10/2/2020)
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (3/3/2015)
- 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA (12/23/2020)
- 114VA10, The Revenue Program–Billing and Collection Records – VA (1/25/2021)

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 five 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/Contracting Officer's Representative (COR) authorizes, documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. Individual training records are retained for seven years. This documentation and monitoring is performed through the use of VA's Talent Management System (TMS). MyVA Electronic Permission Access System (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. CC–CCRS–VAEC–AWS 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, Business Associate Agreement (BAA), or a Non–Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

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

Contractors working on CC–CCRS–VAEC–AWS, usually referred as "contracted employees",

will not be accessing any CC–CCRS–VAEC–AWS information. Contractors provide support to the system and development and implementation but do not handle data within the system. There is no requirement for contractors' signatures on Non–Discloser Agreements (NDA) or confidentiality agreements. Contractor access is verified through the VA personnel Contracting Office Representative (COR) via an Electronic Permission Access System (ePAS) request before access is granted to any contractor. Contracts and contractor access are reviewed annually by the COR(s). The contractors who provide support to the system are required to complete, before access is granted and annually, the following classes in TMS: VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176), Privacy and HIPAA Training (VA 10203) and Information Security and Privacy Role–Based Training for System Administrators (VA 1357076). All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role (T2 or T4 clearances). Contractors with systems administrative access are required to annually complete an 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/contractors must complete annual Privacy and Info Security training, HIPAA training and applicable role–based 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 is based on the role of the user and includes, but is not limited to, the following:

VA 1016925: Information Security and Privacy Role–Based Training for Software Developers (WBT)
VA 3197: Information Security and Privacy Role–Based Training for IT Specialists
VA 4481886: Information Security and Privacy Role–Based Training for Staff in Non–Technical Roles (WBT)

VA 1357076: Information Security and Privacy Role–Based Training for System Administrators
VA 64859: Information Security and Privacy Role–Based Training for Acquisition Personnel (WBT)
VA 1337064: Information Security and Privacy Role–Based Training for Facilities Engineers (WBT)
VA 1357084: Information Security and Privacy Role–Based Training for Data Managers (WBT)
VA 64899: Information Security and Privacy Role–Based Training for IT Project Managers (WBT)
VA 3197: Information Security and Privacy Role–Based Training for IT Specialists (WBT)
VA 1357083: Information Security and Privacy Role–Based Training for Network Administrators (WBT)
VA 1357076: Information Security and Privacy Role–Based Training for System Administrators (WBT)
VA 3867207: Information Security Role–Based Training for Information System Owners (WBT)

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

CC–CCRS–VAEC–AWS Security Plan is completed and documented in eMASS, dated July 2, 2022.
This system received an Authority to Operate on March 24, 2022, with an Authorization Termination Date of Sept 20, 2022.
Risk Review was completed March 22, 2022
System categorization is Moderate.

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL–1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

CC–CCRS–VAEC–AWS is platform as a service (PaaS) hosted by VA Enterprise Cloud (VAEC–AWS).

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

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

NA

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.

NA

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.

NA

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).

NA

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Michael D Hartmann 1612370

Digitally signed by Michael D Hartmann 1612370
Date: 2022.09.30 07:24:54 -06'00'

Privacy Officer, Michael Hartmann

Amine Messaoudi 1136390

Digitally signed by Amine Messaoudi 1136390
Date: 2022.09.30 13:12:13 -05'00'

Information System Security Officer, Amine Messaoudi

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2022.09.30 15:36:44 -05'00'

Information System Owner, Christopher Brown

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):

- Department of Veterans Affairs Veterans Health Administration NOTICE OF PRIVACY PRACTICES
- 23VA10NB3, Non–VA Care (Fee) Records – VA (7/30/2015)
- 24VA10A7, Patient Medical Records – VA (10/2/2020)
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (3/3/2015)
- 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA (12/23/2020)
- 114VA10, The Revenue Program–Billing and Collection Records – VA (1/25/2021)