Privacy Impact Assessment for the VA IT System called:

Non-Community Care Network

Veterans Affairs Central Office (VACO)

Financial Healthcare Service (FHS)

2376

Date PIA submitted for review:

12/10/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Morla D. Roberts	Morla.Roberts@va.gov	512-296-9379
Information System Security Officer (ISSO)	Ronald Murray	Ronald.Murray2@va.gov	512-460-5081
Information System Owner	Jonathan Lindow	Jonathan.Lindow@va.gov	512-981-4871

Abstract

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

Non-Community Care Network (Non-CCN) was formed when Financial Services Center (FSC) procured Commercial Off the Shelf (COTS) software Electronic Claims Adjudication and Management System (eCAMS) designed to adjudicate medical claims. This eCAMS COTS product will serve as the FSC healthcare claims adjudication enterprise solution. This software will become the primary system used by the FSC to adjudicate healthcare claims for FSC customers and will replace existing legacy systems currently used at FSC for this purpose.

Overview

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

1 General Description

A. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

FSC uses eCAMs to processes medical claims from Non-Community Care Network, National Dialysis Service Contract and Camp Lejeune Family Member Program. Claims will be imported, adjudicated and then either approved for payment or denied. Currently In-Network Claims are processed by external organizations.

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

VA owned and VA operated.

2. Information Collection and Sharing

C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?

Over 27.5 million records are stored in support of processing medical claims for veterans and members of the public.

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

D. What is a general description of the information in the IT system and the purpose for collecting this information?

Non-Community Care Network (Non-CCN) collects and processes Health Care Administration information to adjudicate medical claims in support of Non CCN, DNC and CLFMP. Claims will be imported, adjudicated and then either approved for payment by Treasury or denied.

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

Information is shared with VA Office of Integrated Veteran Care (IVC) via the Corporate Data Warehouse (CDW) and Product Integration Tool (PIT) for auditing and quality assurance.

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

Non CCN has a read-only provider portal where providers can access their claim status and amount paid.

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

Non-premise at the Austin Information Technology Center (AITC), and a few servers hosted in the VAEC AWS GoveCloud. All data is maintained in the on-premises systems and any data that is transmitted to VAES AWS GovCloud servers is protected with encryption.

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

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

13VA047 - Individuals Submitting Invoices-Vouchers for Payment – VA

23VA10NB3 - Non-VA Care (Fee) Records-VA

H. What is the SORN?

13VA047 - Individuals Submitting Invoices-Vouchers for Payment – VA
23VA10NB3 - Non-VA Care (Fee) Records-VA

I. SORN revisions/modification

One of the SORNs listed is more than 6 years old and is in the progress of being revised.

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

Yes, 13VA047 applies to -Non-CCN and references VAEC Cloud usage.

4. System Changes

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

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

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

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Other PII/PHI data elements:
Subscriber ID
Group Number Insured SSN
Vendor ID
Vet ID
Patient Control Number (PCN)
Date of Service/Medical Care
Date of Birth
Age
Zip Code
Diagnostic Code
Procedure Code w/ Modifier
Procedural Codes
Prior Medical Authorization Number and Services
Provider Tax ID Number

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

Provider Address: Claim Processing
Referring Provider
Type of Service
Authorization Begin Date
Authorization End Date
Date of Death
Patient Account Number
Patient Eligibility Documentation
Other Health Insurance
Medical Record Number
Computerized Patient Record System (CPRS) Consult Number
CPRS Date of Initial Onset of Dialysis
Referral Request Date
Unique Entity Identifier (UEI)
Billed and Net Payable Amounts
Facility Type
Facility Address

1.2 List the sources of the information in the system
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

The system processes medical claims. Information provided by VA files/databases, required information to process medical claims. Explanations of benefits (EOB) are provided to the medical providers for each claim received at the FSC.

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

VA files/Databases, including eligibility data from Administrative Data Repository (ADR), provide information to process their program specific medical claims.

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

At the completion of the claims process, an Explanation of Benefits (EOB) that explains which claims were paid or denied is sent to the patient and to the provider who submitted the claim.

1.3 Methods of information collection
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

through technologies or other technologies used in the storage or transmission of information in identifiable form?

Most of the information is received via electronic transmission from another system; eligibility data from Administrative Data Repository (ADR).

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

The information is not collected on a form and is not subject to the Paperwork Reduction Act.

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

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

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Received via electronic transmission from another system; eligibility data from Administrative Data Repository (ADR). Validation is performed to validate the services identified by the service provider matches the information contained in the authorization. The Program Integrity Team (PIT) also checks the claims for duplication and matching accuracy with services rendered and service paid.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

The system does not access a commercial aggregator of information.

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

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

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.
(https://www.oprm.va.gov/privacy/systems_of_records.aspx).
13VA047 - Individuals Submitting Invoices-Vouchers for Payment – VA
23VA10NB3 - Non-VA Care (Fee) Records-VA>>

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Sensitive Personal Information including personal contact information, medical information, service information and benefit information may be released to unauthorized individuals.

Mitigation: Non-CCN adheres to information security requirements instituted by the VA Office of Information Technology (OIT). Non-CCN relies on information previously collected by the VA from the individuals. Both contractor and VA employees are required to take Privacy, HIPAA, and information security training annually. The system undergoes complete Web Application Security Assessment (WASA) scans and are not allowed to operate with critical findings. The applications have improved their user validation practices and procedures to ensure user access is authorized. Users are authorized through Form 9957 process.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
<<Name>>	File Identification purposes	To identify individual patient
Full Name	To identify individual patient	
Social Security Number	To identify individual patient	
Age	To identify individual patient	
Personal Mailing Address	To determine travel miles	
Zip Code	To determine travel miles	
Phone Number	To identify individual patient	
Patient Control Number (PCN)	To identify individual patient	To identify individual patient
Gender	To identify individual patient	
Date of Service	To search for specific claims	To search for specific claims
Diagnostic Code	To validate specific claims	
Integrated Control Number (ICN)	To identify specific claims	
Procedure Code w/ Modifier	To search for specific claims	
Provider Address	To determine travel miles	
Provider Tax ID	To identify the provider	To identify the provider
Prior Medical Authorization Number and Services	To identify individual patient	
Type of Service	To determine authorization	
Referring Provider	Authorization tracking	
Date of Death	Auditing	
CPRS Consult Number	Claim tracking	
Referral Request Date	Claim verification	
Other Health Insurance	Authorizing Payment	
Subscriber ID	To identify the correct subscriber	
Group Number Insured SSN	To identify the correct group	
Vendor ID	To identify the correct vendor	
Vet ID	To identify the correct Veteran	
Patient Eligibility Document	For authorization	
Patient Account Number	To identify the claim series	To identify the claim series
CPRS Date of Initial Onset of Dialysis	Claim tracking	
Authorization Begin Date	Claim tracking	
Authorization End Date	Claim tracking	
UEI-(Unique Entity Identifier)	Authorization	
Facility Type	Check authorization for claim	Check authorization for claim
Facility Address	Check travel mile	Search criteria

2.2 Describe the types of tools used to analyze data and what type of data may be produced.

These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

The limited analysis of the data is used to determine eligibility and claim payment. The system generates an Explanation of Benefits (EOB) and an Explanation of Payments (EOP) that explains which claims were paid or denied.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

EOBs and EOPs are sent to the patient and to the provider submitting the claim. This data is tied to the patient record as a data string.

2.3 How the information in the system is secured.
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

All the applications data are protected through encryption 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? (refer to PTA question 3.8).

Social Security Numbers are masked in the Claims UI, only showing the last 4 and they are encrypted at-rest and in-transit.

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

Role	FSC/IVC?	Role Type	Use Case
Provider Reviewer	FSC Role	Configuration	Role used to establish and manage Tax ID providers in eCAMS. Role is limited to creating provider records for the purpose of claims adjudication, not creating vendor records for the purpose of payment.
System Administrator	FSC Role	Admin	Role used by the System Administrator to access the Admin screens and Admin menu to ensure the system is up and running as appropriate

Help-Desk-Org Unit Access	FSC Role	User Admin	Role allows Help Desk staff the ability to assign additional organizational units for users with existing roles and access.
User and Maint Access Admin	FSC Role	Configuration	Role used by configuration specialist to configure, update, and maintain user role profiles.
Read Only	FSC or IVC Role	Read Only	Role allows user a limited read only access to claims and claim related data.
Configuration Specialist	FSC Role	Configuration	Role used by configuration specialist to configure contracts, error codes, duplicate logic, fee schedules, referential data, business rules and any other configuration changes required in eCAMS.
Claims Supervisor	FSC Role	Claims Processor	Role used by Claims Operations Supervisor which includes all Claims Processor Lead capabilities plus some additional functionality such as bulk management of more than 100 claims.
Claims Processor Lead	FSC Role	Claims Processor	Role used by Claims Processor Lead which includes all Claims Processor capabilities plus some additional functionality such as resurrecting or adjusting claims.
Claims Processor	FSC Role	Claims Processor	Role used by Claims Processor staff allowing basic claim processing capability to review claims and claim related data and resolve pended claims. This is an entry level role and cannot perform any additional functions granted to the next higher role.
IVC Manager	IVC Role	Claims Processor	Role allows IVC Manager the IVC Claims Processor Lead capabilities plus some additional functionality such as assignment of claims to users and organizational units.
IVC Claims Processor Lead	IVC Role	Claims Processor	Role allows IVC Claims Processor Lead the IVC Claims Processor 2 capabilities plus access to IVC organizational units and resurrection of claims.
IVC Claims Processor 2	IVC Role	Claims Processor	Role allows IVC Claims Processor 2 the IVC Claims Processor 1 capabilities plus ability to deny and release multiple claims at once and allows direct data entry of claims.

IVC Claims Processor 1	IVC Role	Claims Processor	Role allows basic claim processing capability to review claims and claim related data and resolve pended claims. This is an entry level role and cannot perform any additional functions granted to the next higher role.
IVC Clinical Reviewer	IVC Role	Claims Processor	Role allows IVC Clinical Reviewer access to the Clinical Reviewer organizational unit and the same access as the IVC Claims Processor 2 capabilities except for the ability to resurrect claims.
IVC Bene Travel	IVC Role	Claims Processor	Role allows IVC Bene Travel user access like the IVC Claims Processor 2 but with access to the bene travel organizational unit; no resurrection capability; cannot mass force or mass deny.
IVC Bene Travel Lead	IVC Role	Claims Processor	Role allows IVC Bene Travel user access like the IVC Claims Processor 2 but with access to the bene travel organizational unit; includes the capability to resurrect claims; cannot mass force or mass deny.
Claim Adjustments	FSC or IVC Role	Claims Processor	Role allows user to adjust claims and provides limited read only access to claim data.
ePP Provider User	ePP Role	External Provider	Role allows user to access claims, remittance and EOP pages for claims they have permission to access.
eCAMS Customer Support	FSC or IVC Role	Provider Support	Role allows help desk staff to see payment and EOP details to support provider portal related inquiries.
ePP Provider Administrator	ePP Role	External Provider	Role allows user to execute account management responsibilities such as create ePP Provider Users, add domains and NPIs to ePP,and associate those domains and NPIs to Provider Users. This user may also lock user accounts and expire and unexpired users.
IVC Authorization	IVC Role	Authorization Processor	Role allows user to add authorization related notes to a claim and refer claims to another org unit.

Report Admin	FSC Role	Configuration	Role allows user access to the report module where reports can be defined and scheduled.
IVC Administrative	IVC Role	Configuration	Role allows user to assign a Station and User Location to individual users. This data is used for tracking, training, and workload purposes, not for claims access within eCAMS.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Non-CCN controls access through their built-in user management functions based upon roles. Authorization is granted after a user submits a 9957 and has it approved by their manager, and the application admin.

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

Non-CCN has procedures for granting access utilizing 9957s for authorization.

2.4c Does access require manager approval?

Yes, access requires manager approval.

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

Yes, application logs are sent to SEIM.

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

The application owner.

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*

Name
Social Security Number
Personal Mailing Address
Personal Phone Numbers
Personal Email
Patient Control Number (PCN)
Date of Service/Medical Care
Age
Gender
Zip Code
Diagnostic Code
Procedure Code w/ Modifier
Procedural Codes
Prior Medical Authorization Number and Services
Provider Tax ID Number
Provider Address: Claim Processing
Referring Provider
Integrated Control Number (ICN)
Type of Service
Authorization Begin Date
Authorization End Date
Date of Death
Patient Account Number
Patient Eligibility Documentation
Other Health Insurance
Medical Record Number
Subscriber ID
Group Number Insured SSN
Vendor ID
Vet ID
CPRS Consult Number
CPRS Date of Initial Onset of Dialysis
Referral Request Date
Unique Entity Identifier (UEI)
Tax ID
Billed and Net Payable Amounts

Facility Type
Facility Address

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

Data is retained for 6 years, 3 months as required by General Record Schedule (GRS) Accountable Officers' Accounts Records for each claim as they are recorded separately.

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

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

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

Yes

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

General Record Schedule (GRS) 6: Accountable Officers' Accounts Records, which is governed by Government Accountability Office (GAO) regulations on retention of payment related records. https://www.archives.gov/files/about/records-schedule/nara-records-schedule-list.pdf

3.4 What are the procedures for the elimination or transfer of SPI?

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

6 years 3 months as required by GRS 6 Item 1a. Records Officer and Records Liaison Officer comply with VA Handbook 6300.1 Chap 6, Section 3. We are also finalizing procedures to automate the destruction of media at the appropriate time based on published NARA and VA instructions. Paper records are shredded by a local shredding company weekly.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training, and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

We do not use PII data for testing or training purposes. The only data that is being used is mock data. Since the data is made up, we do not risk PII data. By exception for User Acceptance Tests (UAT's), production data may be used to test in a pre-production environment. After the test the production data is removed.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

Privacy Risk: If information is retained longer than specified, privacy information may be released to unauthorized individuals.

Mitigation:
• HCPS adheres to information security requirements instituted by the VA Office of Information Technology (OIT)
• Both contractor and VA employees are required to take Privacy, HIPAA, and information security training annually.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a **Non-CCN** consists of **5** key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Non-CCN** and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
eCAMS	Yes	Yes	• Full Name • Social Security Number (SSN) • Provider Tax ID Number • Integrated Control Number (ICN) • Date of Birth • Age • Date of Death • Mailing Address • Zip Code • Phone Number • Patient Account Number •Patient Eligibility Documentation	To accurately process claims	Database: Only authorized users have access to the physical database and databases are encrypted to prevent unauthorized modification of the data at rest.

			• Other Health Insurance • Gender • Prior Medical Authorization • Number and Services • Diagnostic Codes • Dates of Service/Medical Care • Procedural Codes • Medical Record Number • Provider ID • Claim Number • Patient Control Number		
Server 1			• First Name • Last Name • Middle Name • SSN • Gender • Phone Number • Address (City, State, Zip Code) • Date of birth • Insurance Coverage Type Coverage Status • Policy Effective Date • Insurance Expiration Date • Insurance Company • Insurance Company ID • Subscriber ID • Group Number Insured SSN • Vendor Name Vendor Address		Only authorized users have access to the physical database and databases are encrypted to prevent unauthorized modification of the data at rest.

			• Vendor Routing Number • Vendor Account Number		
Server 2			• Patient control number • SSN • First name • Last Name • DOB • Tax ID		Only authorized users have access to the physical database and databases are encrypted to prevent unauthorized modification of the data at rest.
Server 3			• Patient control number • SSN • First name • Last Name • DOB • Tax ID		Only authorized users have access to the physical database and databases are encrypted to prevent unauthorized modification of the data at rest.
Server 4			• Patient control number • SSN • First name • Last Name • DOB • Tax ID		Only authorized users have access to the physical database and databases are encrypted to prevent unauthorized modification of the data at rest.

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

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

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

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

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

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

Data Shared with Internal Organizations

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Veterans' Health Administration/CDW	Purpose is for medical claims processing	• Full Name • Social Security Number • Date of Birth • Gender	Sequel Server Integration Services (SSIS) package to read the data using SSL/TLS
Veterans' Health Administration/CDW Other Health Insurance (OHI)	Purpose is for medical claims processing	• Date of Birth • Social Security Number	SSIS package to read the data using SSL/TLS
Veterans' Health Administration	Purpose is for medical claims processing	• Full Name • Social Security Number (SSN) • Integrated Control Number (ICN) • Date of Birth • Age • Date of Death	SSIS package to write the data using SSL/TLS

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
		• Mailing Address • Zip Code • Phone Number • Patient Account Number • Patient Eligibility Documentation • Other Health Insurance • Gender • Prior Medical Authorization Number and Services • Diagnostic Codes • Dates of Service/Medical Care • Procedural Codes • Medical Record Number	
Veterans Health Administration/Master Veteran Index (MVI)	Purpose is for medical claims processing	• Full Name • Social Security Number • Date of Birth • Gender • Address	HTTPS Webservice to retrieve data from MVI
Community Care Referral Authorization (CCRA)/ Health Service Referral System (HSRM)	Purpose is for medical claims processing	• Full Name • Social Security Number • Date of Birth • Gender	Webservice to receive data from HSRM using SSL/TLS
Veterans Health Administration/VHA Support Service Center (VSSC)	Purpose is for medical claims processing	• Social Security Number	sFTP solution to send and receive data from VSSC
Veterans Health Administration/Enrollment System (ES)	Purpose is for medical claims processing	• Full Name • Social Security Number • Date of Birth • Gender	HTTPS Webservice to
Financial Management System (FMS)/Payment History Data	Purpose is for medical claims processing	• VendorId • Name • VetId • VetName • Address • VendorCode	sFTP File import

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Financial Management System (FMS) Vendor Data	Purpose is for medical claims processing	• VendorName • Address1 • Address2 • City • Address • SSN • Phone • Tax ID • Bank Routing Number • Bank Name • GRPBilling Information • Bank Account Type • Vendor Name Cross Reference • Bank Account Number • Customer Reference Number • Email Address	sFTP File import

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions in this section.).

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

Follow the format below:

Privacy Risk: Sensitive Personal Information including personal contact information, service information and benefit information may be released to unauthorized individuals.

Mitigation:

• HCPS adheres to information security requirements instituted by the VA Office of Information Technology (OIT).
• Both contractor and VA employees, including those at VHA/CBO, are required to take Privacy, HIPAA, and information security training annually.
• All employees with access to Veteran's information are required to complete the VA Privacy and
• Information Security Awareness training and Rules of Behavior annually

• Information is shared in accordance with VA Handbook 6500.

Section 5. External Sharing/Receiving and Disclosure

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

5.1 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

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

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

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

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

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

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

Data Shared with External Organizations

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

			more than one)	
Non-Network Providers	Purpose is for medical claims processing	• Name (first, last, middle) • Claim Number • Patient Control Number • Dates of Service • Provider Tax ID • Social Security Number • Billed and Net Payable Amounts • Diagnostic Codes • Email Address • Provider ID (NPI) • Work Phone Number • Date of Birth • Procedure Code with Modifier • Facility Type • Facility Address	SORN 13VA047 SORN 23VA10NB 3	HTTPS TLS

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: PII or PHI could be compromised and used for nefarious purposes.

Mitigation: VA employees and contractors follow procedures designed to mitigate risk of PII/PHI falling into the wrong hands. Annual training along with restrictive access processes greatly reduces the risk of information being compromised. CCNNC Provider Portal is read-only, and providers are validated via SAM.gov account verification along with requiring knowledge of specific claim information.

Section 6. Notice

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

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

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

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

Yes, written notice is provided to each individual when they elect to receive care from the VA. Information disclosure is mandatory; benefits will not be paid unless subject's information is obtained and used to process the medical claims. Individuals are not directly asked to consent to this use of their information. However, they may choose to remove consent. Removal of consent may result in denial of claims or benefits.

6.1b If notice was not provided, explain why.

If an individual wishes to remove consent for a particular use of their information, they should contact the nearest VA Regional Office, a list of where can be found at: https://www.benefits.va.gov/benefits/offices.asp

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

Notice provides purpose and need for information.
https://www.oprm.va.gov/privacy/resources_privacy.aspx

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

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

Information disclosure is mandatory; benefits will not be paid unless subject's information is obtained and used to process the medical claims.

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.

Information disclosure is mandatory; benefits will not be paid unless subject's information is obtained and used to process the medical claims. Individuals are not directly asked to consent to this use of their information. However, they may choose to remove consent. Removal of consent may result in denial of claims or benefits. If an individual wishes to remove consent for a particular use of their information, they should contact the nearest VA Regional Office, a list of where can be found at: https://www.benefits.va.gov/benefits/offices.asp

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. (Work with your Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

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

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

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

Privacy Risk: Veterans and members of the public may not know VA maintains, collects and store data.

Mitigation:
• FSC mitigates this risk by clarifying CCNNC' role through this PIA and the SORNs covering the systems which interact with CCNNC. Individuals upon are request are referred to the source system owner or sponsor, etc.
• Information will not be obtained prior to written notice being provided to everyone.
• Benefits will not be paid unless subject's information is obtained and used to process the medical claims.

Section 7. Access, Redress, and Correction

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

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

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

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

Individuals may access their information via FOIA and Privacy Act procedures. To submit an official FOIA or Privacy Act Request, individuals are providing the contact information for the FSC Privacy/FOIA Officer

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

We do not have any access provision of the Privacy Act

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

This system adheres to the Privacy Act.

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

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

Procedures and contact information for correcting inaccurate or erroneous information is included on the EOB provided to the patient. • Payment was made in accordance with Title 38 U.S.C. 1787 and is considered payment in full. You have the right to appeal any denial on this notice by sending a copy of this EOB, with a written letter of dispute, to the VA Medical Center (VAMC) authorizing this care. Appeals must be received within one year of the date of this EOB. • For Providers: https://eauth.va.gov/accessva/?cspSelectFor=ecamsproviderportal allows providers to access Dialysis-related data online. For claim status and payment information, visit us at https://eauth.va.gov/accessva/?cspSelectFor=ecamsproviderportal or email

vafschcps@va.gov. • For information regarding the VA reconsideration process, please visit the following website: www.va.gov.

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 are made aware of the procedures for correcting his/her information through the notice at collection. • Procedures and contact information for correcting inaccurate or erroneous information is included on the EOB provided to the patient. • Payment was made in accordance with Title 38 U.S.C. 1787 and is considered payment in full. You have the right to appeal any denial on this notice by sending a copy of this EOB, with a written letter of dispute, to the VA Medical Center (VAMC) authorizing this care. Appeals must be received within one year of the date of this EOB. For Providers: • For information regarding the VA reconsideration process, please visit the following website: www.va.gov.

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

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

• Veterans can correct/update their information online via the VA's eBenefits website.
• https://benefits.va.gov/benefits/offices.asp

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: Inaccurate data may be used to process claims.

Mitigation: FSC verifies claim information data against medical authorizations; FSC relies on the data collected by VHA and has clear redress procedures in place. See the PIAs at Privacy Service for Veterans Health Information Systems and Technology Architecture (Vista), Computerized Patient Record System (CPRS), and eBenefits for the VA's mitigation efforts. Data is collected from VHA to accurately process medical claims in accordance with SORN 13VA047.

Section 8. Technical Access and Security

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

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

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

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

• Individuals must take and pass training on Privacy, HIPAA, information security, and government ethics. • Individuals must have a completed security investigation.
• Once training and the security investigation are complete, a request is submitted for access. Before any access is granted, this request must be approved by the supervisor, Information Security Officer (ISO), and OIT.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

There are no users from other agencies for Non-CCN.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Role	FSC/IVC?	Role Type	Use Case
Provider Reviewer	FSC Role	Configuration	Role used to establish and manage Tax ID providers in eCAMS. Role is limited to creating provider records for the purpose of claims adjudication, not creating vendor records for the purpose of payment.
System Administrator	FSC Role	Admin	Role used by the System Administrator to access the admin screens and Admin menu to ensure the system is up and running as appropriate
Help-Desk-Org Unit Access	FSC Role	User Admin	Role allows Help Desk staff the ability to assign additional organizational units for users with existing roles and access.
User and Maint Access Admin	FSC Role	Configuration	Role used by configuration specialist to configure, update, and maintain user role profiles.
Read Only	FSC or IVC Role	Read Only	Role allows user a limited read only access to claims and claim related data.
Configuration Specialist	FSC Role	Configuration	Role used by configuration specialist to configure contracts, error codes, duplicate logic, fee schedules, referential data, business rules and any other configuration changes required in eCAMS.
Claims Supervisor	FSC Role	Claims Processor	Role used by Claims Operations Supervisor which includes all Claims Processor Lead capabilities plus some additional functionality such as bulk management of more than 100 claims.
Claims Processor Lead	FSC Role	Claims Processor	Role used by Claims Processor staff allowing basic claim processing capability to review claims and claim related data and resolve pended claims. This is an entry level role and cannot perform any additional

			functions granted to the next higher role.
IVC Manager	IVC Role	Claims Processor	Role allows IVC Manager the IVC Claims Processor Lead capabilities plus some additional functionality such as assignment of claims to users and organizational units.
IVC Claims Processor Lead	IVC Role	Claims Processor	Role allows IVC Claims Processor Lead the IVC Claims Processor 2 capabilities plus access to IVC organizational units and resurrection of claims.
IVC Claims Processor 2	IVC Role	Claims Processor	Role allows IVC Claims Processor 2 the IVC Claims Processor 1 capabilities plus ability to deny and release multiple claims at once and allows direct data entry of claims.
IVC Claims Processor 1	IVC Role	Claims Processor	Role allows basic claim processing capability to review claims and claim related data and resolve pended claims. This is an entry level role and cannot perform any additional functions granted to the next higher role.
IVC Clinical Reviewer	IVC Role	Claims Processor	Role allows IVC Clinical Reviewer access to the Clinical Reviewer organizational unit and the same access as the IVC Claims Processor 2 capabilities except for the ability to resurrect claims.
IVC Bene Travel	IVC Role	Claims Processor	Role allows IVC Bene Travel user access like the IVC Claims Processor 2 but with access to the bene travel organizational unit; no resurrection capability; cannot mass force or mass deny.
IVC Bene Travel Lead	IVC Role	Claims Processor	Role allows IVC Bene Travel user access like the IVC Claims Processor 2 but with access to the bene travel organizational unit; includes the capability to resurrect claims; cannot mass force or mass deny.

Claim Adjustments	FSC or IVC Role	Claims Processor	Role allows user to adjust claims and provides limited read only access to claim data.
ePP Provider User	ePP Role	External Provider	Role allows user to access claims, remittance and EOP pages for claims they have permission to access.
eCAMS Customer Support	FSC or IVC Role	Provider Support	Role allows help desk staff to see payment and EOP details to support provider portal related inquiries.
ePP Provider Administrator	ePP Role	External Provider	Role allows user to execute account management responsibilities such as create ePP Provider Users, add domains and NPIs to ePP,and associate those domains and NPIs to Provider Users. This user may also lock user accounts and expire and unexpired users.
IVC Authorization	IVC Role	Authorization Processor	Role allows user to add authorization related notes to a claim and refer claims to another org unit.
Report Admin	FSC Role	Configuration	Role allows user access to the report module where reports can be defined and scheduled.
IVC Administrative	IVC Role	Configuration	Role allows user to assign a Station and User Location to individual users. This data is used for tracking, training and workload purposes, not for claims access within eCAMS.

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

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

• Contractors will have access to the system and their contracts are reviewed on an annual basis. • Contractors must take and pass training on Privacy, HIPAA, information security, and government ethics.

• Contractors must have a completed security investigation.

• Once training and the security investigation are complete, a request for access is submitted before any access is granted. This request must be approved by the government supervisor, Information Security Officer (ISO), and Office of Information & Technology (OIT).

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

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

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

NDAs are not used by individual contractors...that is covered in the ROB and protecting PII/PHI training we all take. It's also covered in the contract where there is contract language requiring the vendor to protect PII/PHI.

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.

Talent Management System courses:
VA 10176: Privacy and Info Security Awareness and Rules of Behavior.
VA 10203: Privacy and HIPAA Training
VA 3812493: Annual Government Ethics

8.4 The Authorization and Accreditation (A&A) completed for the system. NO

8.4a If Yes, provide:

1. *The Security Plan Status:* - Approved
2. *The System Security Plan Status Date:* 20 Dec 2023 signed.
3. *The Authorization Status:* Authorized to Operate
4. *The Authorization Date:* 22 Nov 2024
5. *The Authorization Termination Date:* 22 Nov 2025
6. *The Risk Review Completion Date:*16 Oct 2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***
N/A-

Section 9 – Technology Usage

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

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

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

Non-CCN is a Hybrid system with some servers hosted in the Veterans Administration Enterprise Cloud (VAEC) AWS GOVCLOUD. This is an Infrastructure as a Service (IaaS) system.

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

N/A

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.

N/A

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.

N/A

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).

N/A Not using RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

MORLA ROBERTS

Digitally signed by MORLA ROBERTS
Date: 2025.01.03 14:27:03 -05'00'

Privacy Officer, Morla D. Roberts

RONALD MURRAY

Digitally signed by RONALD MURRAY
Date: 2025.01.03 14:18:09 -06'00'

Information System Security Officer, Ronald Murray

JONATHAN LINDOW

Digitally signed by JONATHAN LINDOW
Date: 2025.01.03 12:25:32 -06'00'

Information System Owner, Jonathan Lindow

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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

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

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

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

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)