Privacy Impact Assessment for the VA IT System called:

Healthcare Claims Processing System (HCPS) CLOUD

Financial Services Center (FSC) Veterans Administration (VA)/VACO

Date PIA submitted for review:

8/04/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Frank Samudio Jr.	Frank.Samudio@va.gov	*512-386-2189*
Information System Security Officer (ISSO)	Rito-Anthony Brisbane	Rito-Anthony.Brisbane@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?" and will be published online to accompany the PIA link.

HCPS Cloud is a system-of-systems. As applications move from HCPS to HCPS Cloud, they will be captured in this document. Currently, the only application residing in HCPS Cloud is Community Care Non-Network Claims Provider Portal (CCNNC PP). CCNNC PP provides a read-only means form Non-Network Providers to check claim status and to view explanation of payments (EOP).

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?*

Healthcare Claims Processing System (HCPS) Cloud resides in the Department of Veterans Affairs Enterprise Cloud (VAEC) utilizing Amazon Web Service (AWS). HCPS Cloud's program ownership is in the Financial Healthcare Service, Medical Claims Division. HCPS Cloud contains Community Care Nonnetwork Claims (CCNNC) Provider Portal. The Community Care Non- Network Claims (CCNNC) Electronic Claims Adjudication Management System (eCAMS) Provider Portal Cloud is a read-only means for non-network providers to check claim and payment status and to view explanation of payments (EOPs). CCNNC provides an automated medical claims processing system

from receipt of medical claims documents through claims payment including the appropriate accounting transaction. Expected number of individuals is 10,000. CCNNC is a National System used by providers and medical claim processors outlined above. Information stored in the system includes Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc.), Dates of Service, Service Information, Medical Information such as an Explanation of Payment, and Benefit Information. CCNNC PP is a child to Community Care Non-Network Claims (CCNNC), which resides at the Austin Information Technology Center (AITC). The SORNS applicable to HCPS Cloud (SORN 23VA10NB3 and SORN 13VA047) both require revision. The citation of legal authority: Title 38, United States Code, Section 1703 provides for hospital care and medical services in non-VA Department facilities; Section 1724 provides hospital care, medical services and nursing home care abroad; Section 1725 provides for reimbursement for emergency treatment; Section 1728 provides usual and customary reimbursement of hospital care or medical services of emergency treatment paid for by the Veteran; Section 1781 provides medical care for survivors and dependents of certain Veterans; Section 1802 provides for spina bifida medical coverage; Section 1803 provides for health care to a child of a Vietnam Veteran who suffers from spina bifida; and, Section 1813 provides eligible children health care for covered birth defects or any disability that is associated with those birth defects. It is unlikely that completion of this PIA will result in circumstances that require changes in business processes because this system has implemented security and privacy changes made by other like systems. Being a COTS system, it is not likely that this PIA would result in technology changes.

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)

Claim Number
Patient Control Number
Dates of Service
Billed and Net Payable Amounts
Diagnostic Codes
Procedural Codes with Modifier
Facility Type
Facility Address
Provider ID (NPI)

PII Mapping of Components

CCNNC Provider Portal consists of two components. Each component has been analyzed to determine if any elements of that component collect PII. They type of PII collected by CCNNC Provider Portal and the reasons for collection of the PII are in the table below.

PII Mapped to Components

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
vac10appcnc200	Yes	No	-Name -Claim Number	For providers to check status of claims in a read-only,	Internal protection is managed by access controls such as Multi-

			-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	on-demand inquiry.	Factor Authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.
Vac10appcnc201	**Yes**	**No**	-Name (first, last, middle) -Claim Number -Patient Control Number -Dates of Service	For providers to check status of claims in a read-only, on-demand inquiry.	Internal protection is managed by access controls such as Multi-Factor Authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

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.

CCNNC PP is a subsystem of CCNNC. All information is retrieved from CCNNC Databases.

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 technologies 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.

Information is retrieved from CCNNC databases upon request. Received via electronic transmission from CCNNC; eligibility data from Administrative Data Repository (ADR).

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.

Information presented is a direct draw from eCAMS databases. Only changes would involve masking of partial SSN. When processing medical claims, we check the information in the claim against the veterans' or veterans' family members' eligibility data and the medical authorization provided by VHA. Validation is performed to validate the services identified by the service provider matches the information contained in the authorization. Validation is done to ensure the medical claims being submitted for payment are part of their specified eligibility parameters established at the time they are deemed clinically eligible for the program. The Program Integrity Team (PIT) also checks the eCAMS claims for duplication and matching accuracy with services rendered and service paid.

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

Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111, 501, 1151 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741–1743, 1781, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014.

31 U.S.C. 3512—Executive Agency Accounting and other Financial Management Reports and Plans; Federal Managers' Financial Integrity Act Section 2 of 1982; Federal Financial Management Improvement Act of 1996; E-Government Act of 2002 Title III., Federal Information Security Modernization Act (FISMA) of 2014; Clinger Cohen Act of 1996; 38 CFR part 17 §§ 17.120–17.132; OMB Circular A– 123, Management's Responsibility for Internal Control; and OMB Circular A– 127, Financial Management Systems. SORNS 23VA10NB3 (Non-VA Care (Fee) Records-VA) and 13VA047 (Individuals Submitting Invoices-Vouchers for Payment)-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.

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

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

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

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

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

Follow the format below when entering your risk assessment:
Privacy Risk: If a bad actor accessed CCNNC Provider Portal, then the bad actor may be able to obtain PII and PHI for the patients associated with the account accessed.

Mitigation: Several security measures are being implemented to mitigate the risk of a bad actor accessing PII and PHI via CCNNC Provider Portal:
1.Partial Masking of Social Security Number
2. ID.me or PIV access to program.
3. Manual approval of users.
4. Blocking of common email addresses
5. Logging of user actions
6. Additional security questions required for log-in

CCNNC Provider Portal adheres to information security requirements instituted by the VA Office of Information Technology (OIT) and 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. eCAMS does use the veteran's Social Security Number (SSN) it is masked when used as part of the CCNNC Provider Portal (External Providers). The application uses multi-factor authentication system, ID.me. The system will undergo 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. Application will use System for Award Management (SAM) to further validate authorized users.

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.

Information displayed by CCNNC Provider Portal eCAMS Provider Portal is read-only and allows non-network providers to view claim and payment information associated with claims for which they are authorized access.

Name: Used to identify the patient
Social Security Number: Used as a patient identifier
Date of Birth: Used to identify patient age and confirm patient identity
Mailing Address: Used to contact patient
Zip Code: Used to contact patient
Phone Number(s): Used to contact patient
e-mail address: Used to contact patient
Emergency contact information: Used to contact patient
Certificate License Number: Used to identify provider
Health Insurance Beneficiary Number: Used to identify patient
Financial Account Information: Used to view information on claims
Tax Identification Number: Used to Identify the patient or provider
Information is processed to ascertain eligibility and make medical claims benefits payments.
Diagnosis Codes related to medical conditions: to verify correct service for payment
Dates of Service of medical care: To identify correct claim and service
Billed and Net Payable amounts for medical care: Primary purpose of the portal

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 system doesn't create new information, nor does it modify existing information except for partially masking of the social security number.

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?

Encrypted 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?

SSN is partially masked

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

All employees and contractors are required to participate in general and role-based privacy training annually, all appropriate administrative, technical and safeguards have been implemented to protect CCNNC Provider Portal, data accessed and displayed by the system and users of the system and these controls are reviewed regularly.

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

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> 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. <u>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.</u>

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

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

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.
Add answer here:

• Both contractor and VA employees are required to take Privacy, HIPAA, and information security training annually.
• System of Records Notice SORN is clear about the use of the information, specifically 13VA047 "Individuals Submitting Invoices-Vouchers For Payment-VA (https://www.govinfo.gov/content/pkg/FR-2020-04-23/pdf/2020-08611.pdf)"; 23VA10NB3 "Non-VA Fee Basis Records-VA.(https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf)
• Disciplinary actions: Depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.
• The information is required to process medical claims; without this information, we would not be able to accomplish our mission. Employees requiring access to this system must sign a VA Rules of Behavior (ROB), complete automated annual privacy training and attend classroom training sessions as needed
Users of CCNNC Provider Portal are non-network medical providers and their office representatives. Security and privacy procedures will be followed according to their non-network business rules and regulations. Manual approval of users is granted by the eCAMS helpdesk after the user provides information authenticating user identity. FSC Helpdesk representatives will validate those inbound users are registered in the SAM database and that they are in a list of approved users prior to granting access. Users are only provided access to the claims which they have demonstrated that they are authorized to access.
Users are only given access to PII and PHI that they already have access to. The only information that is new to the provider is the claim and payment status.

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
-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

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.

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

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.

Yes, General Record Schedule (GRS) 6: Accountable Officers' Accounts Records, which is governed by Government Accountability Office (GAO) regulations on retention of payment related records. The retention schedule has been approved by NARA. Link to general records schedule 6.1 below:

https://www.archives.gov/files/records-mgmt/grs/grs06-1.pdf

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

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. 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

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

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

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

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

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

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.

Follow the format below:
Privacy Risk: If information is retained longer than specified, privacy information may be released to unauthorized individuals

Mitigation: CCNNC Provider Portal 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.
• FSC is also finalizing procedures to automate the destruction of media at the appropriate time based on published NARA General Records Schedule 10-1, section, 4.2, Information Access and Protection of Records, dated January 2017 and VA Handbook 6300.1, Records Management Procedures, paragraph 7, dated March 24, 2010.

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***
CCNNC eCAMS	Oracle Real Application Cluster (RAC) Oracle Disaster Recovery (DR)	-Name -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	Compensation and Pension Record Interchange (CAPRI) electronic soft Electronic transmission methods in accordance with VA policy. ware package

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Follow the format below:
Privacy Risk: If a bad internal actor accesses CCNNC Provider Portal information, then they could use the limited PII/PHI to support identity theft activities.

Mitigation: Use of masking, challenge questions, ID.me registration, SAM registration and knowledge of specific claim information combined with manual approval process are used to mitigate risk of a bad actor accessing PII/PHI.

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***
NA	NA	NA	NA	NA

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:
Privacy Risk: N/A

Mitigation: N/A

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.

Yes, written notice is provided to each individual when they elect to receive care from the VA. SORNS 23VA10NB3 (Non-VA Care (Fee) Records-VA) and 13VA047 (Individuals Submitting Invoices-Vouchers for Payment)-VA. https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdfhttps://www.oprm.va.gov/docs/Current_SORN_List_7_1_2022.pdf

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.

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

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

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

Follow the format below:
Privacy Risk: 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 request are referred back to the source system owner or sponsor, etc.
• Information will not be obtained prior to written notice being provided to each individual.
• 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 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.

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

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://www.vahcps.fsc.va.gov/ allows providers to access Dialysis-related data online. For claim status and payment information, visit us at https://www.vahcps.fsc.va.gov/ or email vafschcps@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.

For VA Claims:
• 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.
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.

• Veterans have the ability to correct/update their information online via the VA's eBenefits website.
• http://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.

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

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.
Follow the format below:
Privacy Risk: 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 (Individuals Submitting Invoices-Vouchers for Payment-VA).

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.

• 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.

8.2 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 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 and sign a non-disclosure agreement.

• 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).

8.3 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 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.***

1. The Security Plan Status, - Approved

2. The Security Plan Status Date, - 08-Jul-2021

3. The Authorization Status, - Authorization to Operate (ATO)

4. The Authorization Date, - 17 August 2021

5. The Authorization Termination Date, - 27-Aug-2022

6. The Risk Review Completion Date, - 05-Aug-2021

7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH). – HIGH

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.

Yes 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.

AWS Contract Number NNG15SD22B VA118-17-F-2284

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.

No

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.

AWS is under contract as Cloud Provider in VAEC

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).

no

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 provided in this Privacy Impact Assessment is true and accurate.

FRANK SAMUDIO

Digitally signed by FRANK SAMUDIO
Date: 2022.08.18 16:05:39 -05'00'

Privacy Officer, Frank Samudio Jr.

RITO-ANTHONY BRISBANE

Digitally signed by RITO-ANTHONY BRISBANE
Date: 2022.08.09 14:14:35 -05'00'

Information Systems Security Officer, Rito-Anthony Brisbane

JONATHAN LINDOW

Digitally signed by JONATHAN LINDOW
Date: 2022.08.09 14:11:09 -05'00'

Information Systems 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).

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

https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

https://www.oprm.va.gov/docs/Current_SORN_List_7_1_2022.pdf

https://vaww.oprm.va.gov/docs/PrivacyResources/1605_01_D_2016-08-31.pdf