Privacy Impact Assessment for the VA IT System called:

Healthcare Claims Processing System (HCPS)

Financial Services Center (FSC)

Veterans Administration Corporate Office (VACO)

eMASS ID # 1056

Date PIA submitted for review:

6 FEB 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Mark A. Wilson	Mark.Wilson@va.gov	512-386-2246
Information System Security Officer (ISSO)	Ronald Murray	Ronald.Murray2@va.gov	512-460-5081
Information System Owner	Jonathan Lindow	Jonathan.Lindow@va.gov	512-568-0626

Abstract

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

HCPS is a system of systems comprised of four independent claims processing products. The four products include: 1. Non-Community Care (Non CCN), 2. Other Government Agencies eCAMS (OGA) eCAMS, 3. Camp Lejeune Family Member Program (CLFM) and 4. Veterans Administration Choice (VAC). Each product processes different claim types. Claims are processed for internal VA Integrated Veteran Care (IVC) and external Other Government Agencies (OGA) customers.

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:

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

Healthcare Claims Processing System (HCPS) encompasses four programs utilized for processing medical claims. HCPS resides at the Austin Information Technology Center (AITC) and the program office is in the Financial Healthcare Service, Medical Claims Division. One subcomponent of the CCNNC/eCAMS application, the CCNNC Provider Portal is in the VAEC AWS Cloud.

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

HCPS provides automated and manual medical claims processing systems. From receipt of medical claims documents through claims payment including the appropriate accounting transaction. Expected number of individuals is 100,000. The typical clients are providers, veterans, or family members of eligible veterans, who use one of the four programs included to process and check on claims.

C. Who is the owner or control of the IT system or project?

VA Owned and VA Operated

2. Information Collection and Sharing

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

Over six million medical claims are processed annually. These claims are related to veterans, eligible family members, providers and detainees processed by the Department of Homeland Security (DHS) and Immigrations and Customs Enforcement (ICE).

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

PHI and PII are collected to ensure eligibility and to properly document and pay claims.

F. What information sharing conducted by the IT system? A general description of the modules and subsystems, 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.

G. Is 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?

Only one child component of HCPS is located separately; CCNNC Provider Portal is located in the VAEC AWS Cloud. Rules and measures for protection of PII and PHI are consistent with CCNNC and CCNNC provider Portal.

3. Legal Authority and SORN

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

I.

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. System of Records Notice SORN is clear about the use of the information, specifically 13VA047 “Individuals Submitting Invoices-Vouchers for Payment - VA” and 23VA10NB3 Non-VA Care (Fee) Records.

J. 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?

Yes, 13VA047 applies to CCNNC and references VAEC Cloud usage.

4. System Changes

K. Will the completion of this PIA will result in circumstances that require changes to business processes?

Completion of this PIA will not result in circumstance requiring changes to business processes.

L. Will the completion of this PIA could potentially result in technology changes?

Completion of this PIA will not result in circumstance requiring changes to technology processes.

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. 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
- ☒ 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
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Other PII/PHI data elements:

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

Diagnostic Code
Procedure Code w/ Modifier
Provider Address
Specialty Service
Type of Service
Procedure Description
Referring Provider
CPRS Consult Number
Referral Request Date
Primary Diagnosis Code
Patient History
CPRS Date of Initial Onset of Dialysis
Authorization Begin Date
Authorization End Date
Patient Control Number (PCN)
Date of Service
Subject ID

PII Mapping of Components (Servers/Database)

Health Claims Processing System consists of 25 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 HCPS 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 3.9 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
OGAMEMBERSERVICE	Yes	Yes	Full Name, Claim Number, Patient Control Number, Dates of Service, Provider Tax ID Number,	OGA: These members are detainees that need health checkup and treatment after being detained by ICE.	Internal protection is managed by access controls such as multifactor authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by

			Social Security Number, Diagnosis Procedure Codes		remote access control authenticator, management, audit, and encrypted transmission.
CCNNCPRD	Yes	Yes	Member Info, First Name, Birth Date, Gender, Middle Name, SSN, Address	CCNNC to Adjudicate healthcare claims for FSC customers	Database: Only authorized users have access to physical database and databases are encrypted to prevent unauthorized modification of the date
OgaPaymentManager, OgaPCM, OgaPcmSupport, OgaHcp, Ogaclaim, Ogahcp Aspstate, OgaSupportORR	Yes	Yes	Date of Birth (DOB), First Name, Last Name	OGA: These members are detainees that need health checkup and treatment after being detained by ICE.	Internal protection is managed by access controls such as multifactor authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control authenticator, management, audit, and encrypted transmission.
CLFM, PCDR, PCIS Web	Yes	Yes	DOB, SSN, First Name, Last Name, Middle Name, Address, DOD Insurance	CLFMP Various databases setup to support various FHS application payment process and web interfaces for users to access data.	Internal protection is managed by access controls such as multifactor authentication awareness and training auditing and internal network controls. Remote protection is provided by remote access control, authenticator management, audit

					and encrypted transmission.
PCMCAMPLEJEUNE	Yes	Yes	DOB, SSN, First Name, Last Name, Middle Name, Address, DOD Insurance	These are family members of veterans that were affected by the Camp Lejeune water contamination incident and related health issues.	Internal protection is managed by access controls such as multifactor authentication awareness and training auditing and internal network controls. Remote protection is provided by remote access control, authenticator management, audit and encrypted transmission.
HC Payer	Yes	Yes	DOB, SSN, First Name, Last Name, Middle Name, Address, DOD Insurance	Various FHS programs claim data is staged here for claim load process to load claims into appropriate systems.	Internal protection is managed by access controls such as multifactor authentication awareness and training auditing and internal network controls. Remote protection is provided by remote access control, authenticator management, audit and encrypted transmission.
PCM VACHOICE TW	Yes	Yes	DOB, SSN, First Name, Last Name, Middle Name, Address	VA Choice application adjudication system to adjudicate claims for payment	Internal protection is managed by access controls such as multifactor authentication awareness and training auditing and internal network controls. Remote protection is provided by remote access control,

					authenticator management, audit and encrypted transmission.
PCM VACHOICE HN	Yes	Yes	DOB, SSN, First Name, Last Name, Middle Name, Address	VA Choice application adjudication system to adjudicate claims for payment.	Internal protection is managed by access controls such as multifactor authentication awareness and training auditing and internal network controls. Remote protection is provided by remote access control, authenticator management, audit and encrypted transmission.
Claim Orchestration, FSCOHI, Medical Authorization Services, Medical Member Services, Medical Obligation Services, Medical Provider Services, Medical Vendor Services	Yes	Yes	DOB, SSN, First Name, Last Name, Middle Name, Address	Pay Claims authorized by the office of community care network contract	Internal protection is managed by access controls such as multifactor authentication awareness and training auditing and internal network controls. Remote protection is provided by remote access control, authenticator management, audit and encrypted transmission.
FSC Data Depot	Yes	Yes	Full Name, Claim Number, Patient Control Number, Dates of Service,	These members are detainees that need health checkup and treatment following being detained by ICE.	Internal protection is managed by access controls such as multifactor authentication awareness and training auditing and internal network controls.

			Provider Tax ID Number, SSN, EIN, Diagnosis Code, Procedure Code related to medical condition		Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.
eCAMS VA Staging DB OGA/eCAMS	Yes	Yes	Full Name, Claim Number, Patient Control Number, Dates of service, Provider Tax ID, SSN, EIN, Diagnosis Code, Procedure code related to medical conditions.	These members are detainees that need health checkup and treatment after being detained by ICE.	Internal protection is managed by access controls such as multifactor 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?
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?

Information is provided by veterans, family members, healthcare providers as part of application for treatment and settlement of medical claims. Also provided by DHS and ICE for detainees.

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.

For eligibility and claim processing

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

System doesn't generate privacy information.

1.3 How is the information collected?

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?

Information is received via electronic transmission. Computer to Computer, secure encrypted transfer of information.

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 Camp Lejeune Family Member Program uses VA Form 10-10068 version AUG 2022 (OMB Control Number 2900-0822) since the information is primarily provided by the individual.

1.4 How will the information be checked for accuracy? 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.

Electronic validation is performed upon access to the application to confirm 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 of the request and they are deemed clinically eligible for the program.

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 applications do not use a "commercial aggregator of information."

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

Veterans' Benefits: Title 38, United States Code, Sections 1703, 1724, 1725, 1728, 1781, 1802, 1803, 1813, and Public Law 112-154 which amends title 38, United States Code, to furnish hospital care and medical services to veterans who were stationed at Camp Lejeune, North Carolina, while the water was contaminated at Camp Lejeune. VA Choice was authorized by the Veterans Access, Choice, and Accountability Act of 2014 (Choice Act). The OGA is administered by the MOU in place with Homeland Security. SORN 13VA047, 23VA10NB3 Non-VA Fee Basis Records.

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: 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: Sensitive Personal Information including personal contact information, medical 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). HCPS 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. For our OGA customers, we rely on them to ensure that

personally identifiable information is accurate, complete, and current. The systems 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. All forward-facing portions of HCPS have been removed and placed under separate stand-alone ATOs. All remaining programs under HCPS are internal.

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
Social Security Number	Used as a patient identifier	Not used
Date of Birth	Used to identify patient age and confirm patient identity	Used to identify patient age and confirm patient identity
Mailing Address	Used to contact patient	Used to contact patient
Zip Code	Used to contact patient	Used to contact patient
Phone Number(s)	Used to contact patient	Used to contact patient
Patient-mail address	Used to contact patient	Used to contact patient
Emergency Contact Information	Used to notify Next of Kin	Used to notify Next of Kin
Financial Account Information	Used to pay for claims	Not used
Health Insurance Beneficiary Account Numbers	Used to identify the patient	Used to identify the patient
Certificate/License Numbers	Used to verify the patient	Not used
Tax Identification Number	Used to Identify the patient or provider Information is processed in order to ascertain eligibility and make medical claims benefits payments.	Used to Identify the patient or provider Information is processed in order to ascertain eligibility and make medical claims benefits payments.
Diagnostic Code	for patient processing	Not used
Procedure Code w/ Modifier	for Claim Processing	Not used
Provider Address	for Claim Processing	Not used
Specialty Service	for Claim Processing	Not used
Type of Service	for Claim Processing	Not used
Procedure Description	for Claim Processing	Not used
Referring Provider	for Claim Processing	Not used
CPRS Consult Number	for Claim Processing	Not used
Referral Request Date	for Claim Processing	Not used
Primary Diagnosis Code	for Claim Processing	Not used

Patient History	used to identify patient	Not used
CPRS Date of Initial Onset of Dialysis	for Claim Processing	Not used
Authorization Begin Date	for Claim Processing	Not used
Authorization End Date	for Claim Processing	Not used
Patient Control Number (PCN)	for Claim Processing	Not used
Subject ID	for Claim Processing	Border Patrol Identification of Detainee
Date of Service	for Claim Processing	Not used

2.2 What types of tools are 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. 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.

2.2b 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.

None of the applications under the HCPS ATO use new or previously unutilized information about an individual.

2.3 How is the information in the system 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 applications within HCPS ATO protect data 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?

, those SSNs are masked to all but the VA staff aiding in processing. Each application under the HCPS ATO mask the SSN if used, to all but the VA staff aiding in processing. The data is encrypted in transit and at rest. VA Staff are able to unencrypt.

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 PP, data accessed and displayed by the system and users of the system and these controls are reviewed regularly. In accordance with the OMB Memorandum M-06-15 dated 22 MAY 2006 the HCPS applications use both Dynatrace and Splunk for safeguarding, monitoring, and notification.

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?

Only authorized VA employees and contractors with legitimate need to access information are given permission to access that information. Access control is performed to minimize access to only individuals with need to view the information to perform primary business functions of the applications for processing claims.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes

2.4c Does access require manager approval?

Yes

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

Yes

2.4e Who is responsible for assuring safeguards for the PII?

Security and privacy teams ensure that monitoring tools are in place and that appropriate privacy measures are utilized.

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 Date of Birth Mailing Address Zip Code Phone Numbers Email Address Emergency Contact Information Financial Account Information Health Insurance Beneficiary Account Numbers Certificate/License Numbers Patient eligibility documentation Authorizations for medical care Diagnosis Codes related to medical conditions Dates of Service of medical care Billed and Net Payable amounts for medical care, and Subject ID.

3.2 How long is information retained?

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

Data is retained for 6 years 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)?

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. Please work with the system Privacy Officer and 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, General Record Schedule (GRS) 6: Accountable Officers' Accounts Records, which is governed by Government Accountability Office (GAO) regulations on retention of payment related records.

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

The retention schedule has been approved by NARA.. 6 years 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.

https://www.archives.gov/files/about/records-schedule/nara-records-schedule-list.pdf

nara-records-schedule-list.pdf (archives.gov)

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. Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

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.

The system does 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 ISSO 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: 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: 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.
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 Handbook6300.1, 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***
FSC VL Trader (for OGA)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim processing.	Name Claim Number Patient Control Number Dates of Service Tax ID Vendor ID SSN EIN Diagnosis/Procedural Codes	sFTP encrypted at rest and in transit
FSC File (for OGA)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and	Name Claim Number Patient Control Number Dates of Service Tax ID Vendor ID SSN EIN Diagnosis/Procedural Codes	sFTP encrypted at rest and in transit

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*
	timely medical claim processing.		
Veterans Health Administration/CDW-Other Health Insurance (OHI) (for CCNCC)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim processing.	Date of Birth Social Security Number	SSIS package to read the data using SSL/TLS
Veterans Health Administration/CDW (for CCNCC)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim processing.	Full Name Social Security Number (SSN) Integrated Control Number (ICN) Date of Birth Age Date of Death Mailing Address Zip Code Phone Number Patient Account Number Patient EligibilityDocumentation Other Health Insurance Gender Prior Medical AuthorizationNumber and Services Diagnostic Codes Dates of Service/Medical Care Procedural Codes Medical Record Number	SSIS package to write the data using SSL/TLS
Veterans Health Administration/Master Veteran Index (MVI) (for CCNCC)	Information being shared for purpose of positively identifying the correct claim, payment,	Full Name Social Security Number Date of Birth Gender Address	HTTPS Webservice to retrieve data from MVI

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*
	treatment, provider and patient for accurate and timely medical claim processing.		
Community Care Referral Authorization (CCRA)/ Health Service Referral System (HSRM) (for CCNCC)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim 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 (VSC) (for CCNCC)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim processing.	Social Security Number	sFTP solution to send and receive data from VSSC
Veterans Health Administration/Enrollment System (ES) (for CCNCC)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and	Full Name Social Security Number Date of Birth Gender	HTTPS Webservice to retrieve data from MVI

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*
	timely medical claim processing.		
Financial Management System (FMS)/Payment History Data (for CCNCC)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim processing.	VendorId Name VetId VetName Address VendorCode	sFTP File import
Financial Management System (FMS)/ Vendor Data (for CCNCC)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim 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
Non-CCN (for Heatbeat)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim processing.	CLAIM NUMBER TCN, NAME, MRN, DATE OF BIRTH, GENDER, ADDRESS, DEPENDENT NAME, SOCIAL SECURITY NUMBER, INTEGRATED CONTROL NUMBER, AGE, PHONE NUMBER, PATIENT ACCOUNT NUMBER, OTHER HEALTH INSURANCE, PRIOR MEDICAL	sFTP File import

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*
		AUTHORIZATION NUMBER AND SERVICES, DIAGNOSIS CODES, PROCEDURE CODES, DATES OF SERVICEs	
Financial Management System (FMS) (for PC3)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim processing.	Full Names Date of Birth personal addresses personal email addresses Social security number Date of birth Personal telephone numbers Financial account information Emergency contact information healthcare insurance beneficiary account numbers current medications prior medical authorization number and services previous medical record medical diagnosis codes Medical diagnosis Dates of treatment Physician name and contact information Billed and Payable amounts Physician Name Physician Tax Identification Number Physician National Provider Identifier (NPI) Certificate/License Number Physician Telephone Physician Address	VL Trader
FMS Transaction Service (for PC3)	Information being shared for purpose of positively identifying the correct claim, payment, treatment,	Full Names Date of Birth personal addresses personal email addresses Social security number Date of birth Personal telephone numbers	HTTPS

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*
	provider and patient for accurate and timely medical claim processing.	Financial account information Emergency contact information healthcare insurance beneficiary account numbers current medications prior medical authorization number and services previous medical record medical diagnosis codes Medical diagnosis Dates of treatment Physician name and contact information Billed and Payable amounts Physician Name Physician Tax Identification Number Physician National Provider Identifier (NPI) Certificate/License Number Physician Telephone Physician Address	
Fee Data Service (for PC3)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim processing.	Full Names Date of Birth personal addresses personal email addresses Social security number Date of birth Personal telephone numbers Financial account information Emergency contact information healthcare insurance beneficiary account numbers current medications prior medical authorization number and services previous medical record medical diagnosis codes Medical diagnosis Dates of treatment Physician name and contact information	HTTPS

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*
		Billed and Payable amounts Physician Name Physician Tax Identification Number Physician National Provider Identifier (NPI) Certificate/License Number Physician Telephone Physician Address	
Financial Management system (for PC3)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim processing.	Name Patient Control Number Dates of Service	Shared Folder Path
Dialysis National Contract (for PC3)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim processing.	Name (First and Last) Patient Control Number Dates of Service	SSL Connection
Document Management System (for CLFM)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and	Full Names SSN Date of Birth personal addresses personal email addresses social security number date of birth personal telephone numbers	Web API (via htt

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*
	patient for accurate and timely medical claim processing.	emergency contact information healthcare insurance beneficiary account numbers current medications prior medical authorization number and services previous medical record medical diagnosis codes Medical diagnosis Dates of treatment physician name and contact information Billed and Payable amounts Physician Name, Physician Tax Identification Number/SSN Physician National Provider Identifier (NPI) Certificate/License Number Physician Telephone Physician Address Physician Email Address	
Integrated Financial Acquisition Management System (for OGA eCAMS)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim processing.	Vendor Name Provider Tax ID Number	SSH FTP
Identity Access Management (for OGA eCAMS)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and	SSOi – • Full Name SSOe – • Full Name • SSN • Address • National Provider Identifier (NPI)	Web Agent SSOe-Standard/Junction (Reverse Proxy)

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*
	patient for accurate and timely medical claim processing.		
COTS Package (VL Trader) (for OGA eCAMS)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim processing.	Full Name • Claim Number • Patient Control Number • Dates of Service • Provider Tax ID Number/SSN/EIN	SSH FTP
FTS (FileNet) (for OGA eCAMS)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim processing.	Full Name Claim Number • Patient Control Number • Dates of Service • Provider Tax ID Number/SSN/EIN • Diagnosis/Procedure Codes related to medical conditions	HTTPS
FSC .NET Web Services (for OGA eCAMS)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim processing.	Alien Number • Name • Date of Birth • Gender	HTTPS SOAP or Rest

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document 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 Training 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 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***
Contracted Healthcare Providers through Immigration and Customs Enforcement (ICE) Healthcare Services Corps (IHSC) (for OGA)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim processing.	Name Claim Number Patient Control Number Dates of Service Tax ID Billed and Net Payable amounts SSN EIN Diagnosis/Procedural Codes Vendor ID Subject ID	SLA	HTTPS Via portal
Non-Network Providers (for Non-CCN)	Information being shared for purpose of positively identifying the correct claim, payment, treatment, provider and patient for accurate and timely medical claim 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 Vendor Name Vendor Telephone Vendor Address Vendor ID (TAX ID or SSN)	SLA with Integrated Veteran Care (IVC) SORN 13VA047 SORN 23VA10NB3 Treasury Web Application Infrastructure Interconnection Security Agreement (TWAI IS	HTTPS TLS HTTPS (TLS) from users' (staff) workstation

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: If external agencies fail to protect PII/PHI shared by HCPS systems, information could be shared with bad actors.

Mitigation: Memorandums of Understanding (MOU) are in place with agencies receiving PII/PHI from HCPS systems.

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 6.1 on the last page of the document. Also provide notice given to individuals by the source system (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?

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 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, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Yes, written notice is provided to each individual when they elect to receive care from the VA. System of Records Notice SORN is clear about the use of the information, specifically 13VA047 "Individuals Submitting Invoices-Vouchers For Payment-VA"; routine use is under revision and 23VA10NB3 "Non-VA Fee Basis Records-VA.(https://www.gpo.gov/fdsys/pkg/FR-2009-08-31/pdf/E920911.pdf) Immigration and Customs Enforcement Health Service Corps (IHSC) and Health and Human Services (HHS) are each responsible for providing applicable notices to their patients receiving care as well as providers providing medical services. These patients are not Veterans. SORN 213VA0475A1 "Other Government Agencies-VA" 2023-12395.pdf (federalregister.gov)

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Immigration and Customs Enforcement Health Service Corps (IHSC) and Health and Human Services (HHS) are each responsible for providing applicable notices to their patients receiving care as well as providers providing medical services.

6.1c 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.

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. Camp Lejeune family members can decline to provide the requested information but if any or all the requested information is not provided, it may delay or result in denial of their request for Camp Lejeune Family Member Health Care Program (CLFMP) benefits.

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 request 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

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 System ISSO 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: 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 stores data.

Mitigation: FSC mitigates this risk by clarifying HCPS' role through this PIA and the SORNs covering the systems which interact with HCPS. 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 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?

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 http://www.foia.va.gov/ 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. In order to submit an official FOIA or Privacy Act Request, individuals are providing the contact information for the FSC Privacy/FOIA Officer. VAFSC Privacy Department VAFSCPrivacyDept@va.gov

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)?

Not exempt.

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?

The applications under the HCPS ATO are compliant with the FOIA/Privacy Act best practices.

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. 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: AccessVA allows providers to access Dialysis-related data online. For claim status and payment information, visit us at AccessVA or email vafschcps@va.gov. • For information regarding the VA reconsideration process, please visit the following website: www.va.gov. Specifically, for Camp Lejeune: • Payment was made in accordance with Title 38 U.S.C. 1787 and is considered payment in full. Appeals must be received within two years of the date of this EOB. If you disagree with the payment or decision regarding this medical claim, you need to send a copy of this EOB along with a written reason stating why you disagree with the payment or decision to the following Appeal address: DEPARTMENT OF VETERANS AFFAIRS, Financial Services Center, Camp Lejeune Family Member Program, PO Box 149200 Austin, TX 78714-9200.

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 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:

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

For Camp Lejeune:

•Payment was made in accordance with Title 38 U.S.C. 1787 and is considered payment in full. Appeals must be received within two years of the date of this EOB. If you disagree with the payment or decision regarding this medical claim, you need to send a copy of this EOB along with a written reason stating why you disagree with the payment or decision to the following Appeal address: DEPARTMENT OF VETERANS AFFAIRS, Financial Services Center, Camp Lejeune Family Member Program, PO Box 149200 Austin, TX 78714-9200.

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 have the ability to correct/update their information online via the VA's eBenefits website. http://benefits.va.gov/benefits/offices.asp For DHS & HHS, there are no other formal redress systems in place.

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 System ISSO to complete all Privacy Risk questions inside the document this section).*

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 could 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 for Vista, CPRS, and eBenefits for the VA's mitigation efforts. Data is collected from VHA to accurately process medical claims in accordance with SORN 13VA047 for VA Claims and SORN (213VA0475A1) for IHSC OGA/eCAMS claims.

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?

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?

VA Employees: 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. For external providers, access is granted to individuals withID.me validation, organizational verification, and challenge questions.

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?

External providers and claim processors roles include administrator, with control of enrollment within their healthcare network and basic user with access to claim information for within their authorized area.

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.

External providers have read-only access to claim and payment information. Internal VA and OGA users have access to claim and eligibility information based on varying roles within the applications.

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.• 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? YES

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 23 MAY 2023
3. *The Authorization Status:* Authority to Operate (ATO)
4. *The Authorization Date:* 9 AUG 2023
5. *The Authorization Termination Date:* 9 AUG 2024
6. *The Risk Review Completion Date:* 8 FEB 2023

7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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

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

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.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Yes, System uses VAEC AWS Cloud houses servers from CCNNC Provider Portal.

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). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes, AWS Contract Number NNG15SD22B 36C10B22F0207.

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.

Yes, because this is within 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

ID	Privacy Controls
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

MARK WILSON

Digitally signed by MARK WILSON
Date: 2024.05.07 16:21:54 -05'00'

Privacy Officer, Mark A. Wilson

RONALD MURRAY

Digitally signed by RONALD MURRAY
Date: 2024.05.08 08:36:56 -05'00'

Information Systems Security Officer, Ronald Murray

JONATHAN LINDOW

Digitally signed by JONATHAN LINDOW
Date: 2024.05.08 08:49:28 -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; screen shot of a website collection privacy notice).

HELPFUL LINKS:

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 Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices