Privacy Impact Assessment for the VA IT System called:

Center for Care and Payment Innovation CCPI Cloud Database (CCD)

(CCPI) Office of Healthcare Innovation and Learning (OHIL)

Date PIA submitted for review:

March 14, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Christian Loftus	Christian.Loftus@va.gov	859-281-2470
Information System Security Officer (ISSO)	Karen A. McQuaid	karen.mcquaid@va.gov	708-724-2761
Information System Owner	Michael F. Harry	michael.harry@va.gov	202-425-0307

Abstract

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

The Center for Care and Payment Innovation (CCPI) Cloud Database (CCD) is a cloud-based system that collects both patient and non-patient level data from CCPI pilot programs to facilitate the analytics and reporting of these programs. The data in the CCD is used to provide important pilot Measurement and Evaluation (M&E) data to stakeholders including CCPI leadership, the VA Innovation Steering Subcommittee (ISS), and the United States Congress.

Overview

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

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

The CCPI Cloud Database (CCD) is owned by the VHA Center for Care and Payment Innovation (CCPI) which is part of the Office of Healthcare Innovation and Learning (OHIL).

The business purpose for the creation of the CCD is to allow CCPI to facilitate flexible and concurrent growth using both diverse and dynamic data frameworks as new CCPI pilots are implemented. This strategy will allow CCPI pilots to be faster, more efficient, and more cost effective than would be capable without such a system. As a subsequent benefit, information transparency to VA clients will be improved along with better reporting capabilities. These enhancements will be used to improve ROI and to provide reporting to Congress.

The CCPI Cloud Database (CCD) is VA owned and operated. It is maintained by CCPI and hosted within the AWS portion of the VA Enterprise Cloud (VAEC). The VAEC AWS environment is owned and maintained by the VA Enterprise Cloud Service Office (ECSO).

The expected number of individuals whose information will be stored in the system is approximately 50,000 records in the first year. This number will be dependent on the volume of participants in the pilots and who consent to data sharing.

The CCPI Cloud Database (CCD) is a cloud-based system that collects data [both patient and non-patient level] from CCPI pilot programs for analytics and to facilitate reporting for pilot monitoring and evaluation.

The CCD will accept the in-bound only sharing of external data from partners outside of VA. An example of this is a monthly workbook submission from participating pilot care providers such as VETSmile. This uni-directional data sharing will take place via the system's secure web front-end module which functions to securely ingest the sensitive data for processing and ingestion into the CCD.

The CCD system will be operated from only one site within the VAEC.

The legal authority for the CCD to operate include the following:
- The VA Mission Act of 2018 (Public Law No: 115-182 § 152)
- The Privacy Act of 1974, 5 United States Code (U.S.C.) § 552a
- System of Record Notice (SORN) number 206VA10 - CCPI Cloud Database (CCD)

The completion of this PIA will not result in circumstances that require changes to business processes

The completion of this PIA will not result in technology changes

The existing SORN (206VA10) will be approved by the time this PIA is processed. It is not anticipated that the approved SORN will need modification or revision and re-approval. The current SORN covers both cloud usage and storage.

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)

PII Mapping of Components

The CCPI Cloud Database consists of **two** key components, 1) a collection of serverless applications and 2) a database. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **the CCPI Cloud Database** and the reasons for the collection of the PII are in the Mapping of Components table below.

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**
CDW	YES	YES	Patient ICN Patient First Name Patient Last Name Patient SSN Birth Date Time Gender Self-Identified Gender Race Ethnicity Street Address 1 Street Address 2 City State Zip GIS FIPS Code Employment Status Occupation Hardship Flag Hardship Reason Patient SID (PK) Encounter Date Time Visit SID Patient Visit Reason Unique Visit Number Location SID Service Category Diagnosis Count ICD10 SID Procedure Count	This data is needed to facilitate Pilot Monitoring & Evaluation	VA OIT required Security controls, Advanced Encryption, user Access authorizations managed through a centralized process, Project membership restricted to minimum necessary

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
			CPT Code Admit Date Time		

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.

CCPI Pilot Providers will directly collect data and upload it into the CCD system.
At the time this PIA document was written, CCPI has only a single active pilot called VETSmile. The VETSmile pilot is comprised of nine (9) external organizations who will submit data via the portal:

1) American Dental Association
2) CareQuest Institute for Oral Health
3) CompleteCare Health Network (CompleteCare)
4) Eastern Carolina University of Dental Medicine
5) National Association of Community Health Centers (NACHC)
6) New York College of Dentistry
7) Rutgers School of Dental Medicine
8) VA Office of Dentistry
9) Zufall Health System

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.

After meeting the precondition of Veteran Consent to data sharing, the information is collected by pilot care providers during the course of normal their care for the Veteran.

The collected data is then transmitted through a highly secure web portal using SSL encryption and a secure submission process that places uploads directly into a private cloud staging area where the data is immediately encrypted at rest. The private S3 Staging area will leave the files encrypted where they are processed by the automated ETL process and loaded into the CCPI Cloud Database (CCD) in secure and monitored AWS GovCloud environment within the VA Enterprise Cloud (VAEC).

Although both Personally Identifiable Information (PHI) and Personal Health Information (PHI) are collected and stored. The submitted data will reside within the VA network and only be accessed by approved federal employees or federal contractors who have the necessary security clearance, permissions, and training.

The information is collected on and for the CCD and is NOT subject to the Paperwork Reduction Act.

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.

CCD Data is checked on every submission in order to ensure accuracy. The CCD system does not utilize a commercial aggregator of information to operate or function. The following steps are taken in the check process:
1) The database is designed with data integrity built-in
2) Developers follow a Dev/QA checklist
3) There is a peer review process
4) Users work with pilot teams for acceptance testing and validation.

The CCD system does not utilize a commercial aggregator of information to operate or function

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

The legal authority for the CCD to operate and collect the information it needs is found here:
- The VA Mission Act of 2018 - Public Law No: 115-182 § 152
- The Privacy Act of 1974 - United States Code (U.S.C.) § 552a
- System of Record Notice (SORN) number 206VA10 - CCPI Cloud Database (CCD)

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Privacy Risk: Unauthorized access or disclosure of veteran personally identifiable information (PII) such as name or DOB.

Mitigation: Only the minimum necessary PII is collected to support the functionality of the monitoring, measurement, and evaluation processes of the program. This will also ensure the ability to pipeline Veterans and enhance coordination of care, communication with Veterans in the scenario of a data breach and provide insights directly to Veterans regarding any insight the M&E Team may that that can be useful for individuals.

CCPI's M&E Team will verify and oversee provider process in record keeping and maintenance to ensure that documentation within the EHR system identifies names of veterans that are on their veteran id ensure that PII is accurate. The M&E Team will consider comparing the PII for contact information (address, email, phone number, etc.) that are in covered entities' systems against contact information disclosed in the CDW for data validation and will monitor the percent difference. If implementation of unique id's created for each pilot is successful in cohort and referral models, the Measurement and Evaluation team will be able to successfully find the name in the CDW which will improve data accuracy.

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.

Information received from pilot care providers is used to collect information that provides a better understanding of the aggregate outcomes, costs, and efficacy of individual CCPI pilot programs and provide new insights about these programs.

- Name: Used as Patient Identifier
- Social Security Number: Used as Patient Identifier
- Date of Birth: Used as Patient Identifier
- Personal Mailing Address: Used as Patient Identifier
- Financial Account Information: Used as Patient Identifier
- Previous Medical Records: Used as Patient Identifier
- Gender: Used as Patient Identifier
- Application for care status: Used as EHR data point
- Bad Address Indicator: Used as Data Validation Element
- Catastrophic Disability Reason: Used as EHR data point
- Catastrophic Disability Type: Used as EHR data point
- CDW Possible Test Patient Flag: Used as EHR data point
- Dental Classification: Used as EHR data point
- Dental Eligibility Flag: Used as EHR data point
- Disability Percentage: Used as EHR data point
- Discharge Type: Used as EHR data point
- Eligibility: Used as EHR data point
- Eligibility Status: Used as EHR data point
- Eligibility VA Code: Used as EHR data point

- Enrollment Priority: Used as EHR data point
- Insurance Company: Used as EHR data point
- Insurance Company SID: Used as EHR data point
- Insurance Coverage Flag: Used as EHR data point
- MAS Eligibility Name: Used as EHR data point
- Medicaid Eligible Flag: Used as EHR data point
- Medicaid Number: Used as EHR data point
- Patient Type: Used as EHR data point
- Period Of Service: Used as EHR data point
- Sensitive Flag: Used as EHR data point
- Service Connected Flag: Used as EHR data point
- Test Patient Flag: Used as EHR data point
- Veteran Flag: Used as EHR data point
- Veteran Transportation Program Flag: Used as EHR data point
- Income: Used as EHR data point
- Total Dependents: Used as EHR data point
- Patient SID (PK) : Used as EHR data point
- Hardship Flag: Used as EHR data point
- Hardship Reason: Used as Socio-demographic
- Patient ICN: Used as EHR data point
- Bill Total Charges: Used as Cost data collection
- Admit Date Time : Used as EHR data point
- Admit Diagnosis: Used as EHR data point
- CPT Code: Used as EHR data point
- CPT SID: Used as EHR data point
- Diagnosis Count: Used as EHR data point
- Encounter Date Time: Used as EHR data point
- ICD10SID: Used as EHR data point
- Inpatient Diagnosis SID: Used as EHR data point
- Location SID: Used as EHR data point
- LOS In Service: Used as EHR data point
- Patient Visit Reason: Used as EHR data point
- Procedure Count: Used as EHR data point
- Service Category: Used as EHR data point
- Unique Visit Number: Used as EHR data point
- Visit SID: Used as EHR data point
- Birth Date Time: Used as Patient Identifier

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.

1.

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 CCD will utilize a combination of COTS Data Analysis tools and custom coded queries to analyze the data submitted. The types of analysis the CCD system conducts include Veteran demographic, socio-economic, and clinical care data will be collected and used for the creation of metrics and data analyses for the purposes of aiding in identifying eligible veterans (target populations), monitoring and evaluating success of pilot lifecycles, facility and VISN operations.

The information makes available specific measurements that allow CCPI to fulfill contractual obligations such as showing improvements in quality of care and cost savings, improvements in care coordination, business intelligence reporting, and survey data scoring. Through this, pilots will be enhanced through transparency of quality improvement and process refinements/ key findings through the pilot lifecycle. Further, visualizations/dashboards, metrics and tools will aid the team in refinement of the pilot processes for enhanced strategic capabilities, scalable and efficient models, and business intelligence reporting.

No individual level action will ever be taken against or for the individual identified because of the newly derived data as its purpose is to identify aggregate information, such as target veteran populations.

Any significant insights derived from CCD findings will first be reported to the VA and Congress, and upon feedback from the Secretary, the CCPI will produce reports and insights for Veterans and providers to improve data transparency and awareness.

No new data created by the CCD will be accessible to Government employees to make determinations about any individual under any circumstances.

2.3 How is the information in the system secured?

This question is 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?

CCD system data is encrypted at rest and in transit at or above VA network encryption standards.

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

All data, including PII not limited to SSN's, is protected with encryption at rest and in transmission at or above VA network encryption standards. Supervisory assignment of functional categories restricting employee and contractor access to systems information.

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

CCD system data is encrypted at rest and in transit at or above VA network encryption standards.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

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

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

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

The information that is collected and used in the CCD is the minimum necessary information needed to provide the services under the VA Mission Act of 2018. All employees and contractors with access to Veterans' information are required to complete VA Rules of Behavior and VA Privacy and Security training annually. Disciplinary actions, up to and including termination of employment, are possible for violations of the requirements specified in the training and their positions. Additionally, all access to the information requires a Personal Identity Verification (PIV) card for access.

Access to PII is assigned based on the role of the individual and is detailed by the manager in the user provisioning process. These access rights are removed and reassigned for each transferred user, and these access permissions are re-approved annually through entitlement reviews of the CCD system. Additionally, prior to the entitlement reviews, all access assigned to roles are reviewed and approved by the application owner. All modifications, creations, and deletes are monitored and recorded to an audit table.

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
- Personal Mailing Address
- Financial Account Information
- Previous Medical Records
- Gender
- Application for care status
- Bad Address Indicator
- Catastrophic Disability Reason
- Catastrophic Disability Type
- CDW Possible Test Patient Flag
- Dental Classification
- Dental Eligibility Flag
- Disability Percentage
- Discharge Type
- Eligibility
- Eligibility Status
- Eligibility VA Code
- Enrollment Priority
- Insurance Company
- Insurance Company SID
- Insurance Coverage Flag
- MAS Eligibility Name
- Medicaid Eligible Flag
- Medicaid Number
- Patient Type
- Period Of Service
- Sensitive Flag
- Service-Connected Flag
- Test Patient Flag
- Veteran Flag
- Veteran Transportation Program Flag
- Income
- Total Dependents
- Patient SID (PK)
- Hardship Flag
- Hardship Reason
- Patient ICN
- Bill Total Charges
- Admit Date Time
- Admit Diagnosis
- CPT Code
- CPT SID

- Diagnosis Count
- Encounter Date Time
- ICD10SID
- Inpatient Diagnosis SID
- Location SID
- LOS In Service
- Patient Visit Reason
- Procedure Count
- Service Category
- Unique Visit Number
- Visit SID
- Birth Date Time

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."

Information in the CCD is retained for the life of the CCPI pilot program, plus the NARA required records retention period.

NARA approval of new Records schedule Pending.

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.

Information in the CCD is retained for the life of the CCPI pilot program, plus the NARA required records retention period.

NARA approval of new Records schedule Pending.

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

All records in the CCD are electronic in nature and elimination / destruction involves logical removal from the electronic storage medium. When the storage medium is to be destroyed at the end of its use, physical destruction of underlying physical storage is handled by Amazon as covered by our BAA and detailed in their data destruction policies. This process ensures that date is destroyed in accordance with the Department of Veterans' Affairs Handbook_6500_24_Feb_2021.pdf (https://www.oprm.va.gov/docs/Handbook_6500_24_Feb_2021.pdf)

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

The CCD system does not use PII for testing, training, or research. To avoid the need to use PII or PHI for these purposes, we employ test data generators, data cloners, and data redactors which enable the creation of testing / research & development datasets that mimic the "shape" of real data without containing any PII or PHI

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.

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: Data retained by the system is at risk of unintended access, disclosure, or breach

Mitigation: Only the minimum PII necessary is retained, minimizing the magnitude of harm. Access controls are set in place to limit access automatically and the CCD follows and enforces the principle of least privilege to the degree possible. A suite a technical and process controls are in place to harden the platform and processes as much as possible without impacting business function.

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***
N/A	N/A	N/A	N/A

CCPI Cloud Database (CCD) is a uni-directional data ingestion and analytics system. The information in the CCD is not transmitted or shared after it is received, instead its information will be used to report aggregate data on active CCPI pilot programs.

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: N/A

Mitigation: N/A

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***
American Dental Association (ADA)	Data is needed to facilitate Pilot Monitoring & Evaluation	Socio-demographic Healthcare utilization Financial Information EHR Data	● The VA Mission Act of 2018 - Public Law No: 115-182 § 152 ● The Privacy Act of 1974 - United States Code (U.S.C.) § 552a ● System of Record Notice (SORN) number 206VA10 - CCPI Cloud Database (CCD)	Data submission via .csv
CareQuest Institute for Oral	Data is needed to facilitate	Socio-demographic Healthcare	● The VA Mission Act of 2018 - Public Law No: 115-182 § 152	Data submission via .csv

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*
Health (CareQuest)	Pilot Monitoring & Evaluation	utilization Financial Information EHR Data	● The Privacy Act of 1974 - United States Code (U.S.C.) § 552a ● System of Record Notice (SORN) number 206VA10 - CCPI Cloud Database (CCD)	
CompleteCare Health Network (Complete Care)	Data is needed to facilitate Pilot Monitoring & Evaluation	Socio-demographic Healthcare utilization Financial Information EHR Data	● The VA Mission Act of 2018 - Public Law No: 115-182 § 152 ● The Privacy Act of 1974 - United States Code (U.S.C.) § 552a ● System of Record Notice (SORN) number 206VA10 - CCPI Cloud Database (CCD)	Data submission via .csv
Eastern Carolina University School of Dental Medicine (ECU)	Data is needed to facilitate Pilot Monitoring & Evaluation	Socio-demographic Healthcare utilization Financial Information EHR Data	● The VA Mission Act of 2018 - Public Law No: 115-182 § 152 ● The Privacy Act of 1974 - United States Code (U.S.C.) § 552a ● System of Record Notice (SORN) number 206VA10 - CCPI Cloud Database (CCD)	Data submission via .csv
National Association of Community Health Centers (NACHC)	Data is needed to facilitate Pilot Monitoring & Evaluation	Socio-demographic Healthcare utilization Financial Information EHR Data	● The VA Mission Act of 2018 - Public Law No: 115-182 § 152 ● The Privacy Act of 1974 - United States Code (U.S.C.) § 552a ● System of Record Notice (SORN) number 206VA10 - CCPI Cloud Database (CCD)	Data submission via .csv

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*
New York College of Dentistry	Data is needed to facilitate Pilot Monitoring & Evaluation	Socio-demographic Healthcare utilization Financial Information EHR Data	● The VA Mission Act of 2018 - Public Law No: 115-182 § 152 ● The Privacy Act of 1974 - United States Code (U.S.C.) § 552a ● System of Record Notice (SORN) number 206VA10 - CCPI Cloud Database (CCD)	Data submission via .csv
Rutgers School of Dental Medicine (Rutgers)	Data is needed to facilitate Pilot Monitoring & Evaluation	Socio-demographic Healthcare utilization Financial Information EHR Data	● The VA Mission Act of 2018 - Public Law No: 115-182 § 152 ● The Privacy Act of 1974 - United States Code (U.S.C.) § 552a ● System of Record Notice (SORN) number 206VA10 - CCPI Cloud Database (CCD)	Data submission via .csv
VA Office of Dentistry (VA Dentistry)	Data is needed to facilitate Pilot Monitoring & Evaluation	Socio-demographic Healthcare utilization Financial Information EHR Data	● The VA Mission Act of 2018 - Public Law No: 115-182 § 152 ● The Privacy Act of 1974 - United States Code (U.S.C.) § 552a ● System of Record Notice (SORN) number 206VA10 - CCPI Cloud Database (CCD)	Data submission via .csv
Zufall Health System	Data is needed to facilitate Pilot Monitoring & Evaluation	Socio-demographic Healthcare utilization Financial Information EHR Data	● The VA Mission Act of 2018 - Public Law No: 115-182 § 152 ● The Privacy Act of 1974 - United States Code (U.S.C.) § 552a ● System of Record Notice (SORN) number	Data submission via .csv

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*
			206VA10 - CCPI Cloud Database (CCD)	

The information in the CCD is not to be shared to entities external to VA, instead its information will be used to report aggregate data on active CCPI pilot programs.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Privacy Risk: There is a risk of information retained by the CCD being accessed during the course the sharing of information outside of the CCPI through a security breach.

Mitigation: The CCPI Cloud Database (CCD) has no direct method of external data sharing and the components within the CCD are secured within the VA Enterprise Cloud (VAEC) which implements Federal Risk and Authorization Management Program (FedRAMP) approved security measures. Additionally, access to the system is monitored and restricted to personnel with both Multi-Factor Authentication and assigned permissions. In addition, all data is encrypted at rest using FIPS 140-2 encryption with keys maintained by the AWS KMS service.

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.

Notice is provided and available to each individual at https://www.va.gov/search/?query=VHA%20Notice%20of%20Privacy%20Practice%20(NOPP)&t=false, along with a Patient Data Sharing Consent Form before collection of the information. Data collection only takes place upon consent being given.

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

Individuals have the opportunity and right to decline to provide information or have it collected. There is no penalty or denial of service attached to this action.

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

Each facility participating in a CCPI pilots signs a Memorandum of Agreement (MOA) that outlines the scope of data sharing and planned usage. Veteran's consent to data sharing using facility specific general consent forms that approve data to be shared between the facility and the VA. Veterans can approve or decline consent however they cannot choose which use cases their data will be utilized in. At any time, Veterans can excise their right to change their consent for data sharing and their data will be erased from our database.

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: If notice is not provided in a timely manner, a Veteran may share information that they wish to remain private.

Mitigation: Privacy practice notices are provided to the veteran at the time of service. This is in accordance with (IAW) VHA Handbook 1605.04 Notice of Privacy Practices.

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.

The CCD is designed to be an information gathering system, not for information dissemination. There are no facilities for participants to view their own profile information or case status and related notes. However, most relevant Veteran information in the CCD is pulled from the CDW with their original data coming into the CDW from their VistA EMR. Veterans can request access to their records by submitting a written FOIA request in accordance with M28R, Part III, Section C, Chapter 2.04(b)(c). in accordance with VA policies.

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 are the same as given in 7.1

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.

Veterans are informed of the amendment process by many resources to include the Notice of Privacy Practice (NOPP) which states:

- Right to Request Amendment of Health Information.
- File an appeal
- File a "Statement of Disagreement"
- Ask that initial request for amendment accompany all future disclosures of disputed information

You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in

writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following: Information can also be obtained by contacting the Department of Veterans Affairs Release of Information (ROI) office.

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.

Veterans and other individuals are encouraged to use the formal redress procedures discussed above in Section 7.3 to request edits to their personal medical records and other personal records retained about them.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Privacy Risk: There is a risk that a Veteran may not know how to obtain access to their records or how to request corrections to their records.

Mitigation: As stated in section 7.3, the Notice of Privacy Practice (NOPP), which every patient signs prior to receiving treatment, discusses the process for requesting an amendment to one's records. Beneficiaries are reminded of this information when obtaining a copy of the NOPP. The VA Release of Information (ROI) office is available to assist Veterans with obtaining access to their medical records and other records containing personal information. The Veterans' Health Administration (VHA) established MyHealtheVet

program to provide Veterans remote access to their medical records. The Veteran must enroll to obtain access to all the available features. In addition, Privacy Handbook 1605.1 establishes procedures for Veterans to have their records amended where appropriate

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.

Access to the Veterans Affairs Enterprise Cloud (VAEC) and CCPI Cloud Database (CCD) are restricted to authorized VA employees and Contractors who must complete both the HIPAA and Information Security training. Specified access is granted based on the individual's functional role. Role based training is required for individuals with significant information security responsibilities to include but not limited to System Administrators, Network Administrators, Database Managers, Systems Engineers, Applications Developers and Testers.

Access is requested per VAEC policies utilizing Electronic Permission Access System (ePAS). Users submit access requests based on need to know and job duties. Supervisor and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes.

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.

Only approved and authorized Federal Government Contractors with Signed Non-Disclosure agreements and specifically assigned to CCPI will have access to the CCD and the PII maintained within it. This access may have both a design and maintenance capacity. As a precondition to this access, a background investigation is completed, and the data can only be accessed over the secure VA network using Multi-Factor Authentication.

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.

All individuals with access the CCD's data must complete two VA provided courses on the VA Talent Management System (TMS):

- VA Privacy and Information Security Awareness and Rules of Behavior (TMS 10176)
- Privacy and HIPAA Training (TMS 10203)

8.4 Has Authorization and Accreditation (A&A) been completed for the system? NO

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:* In Process: [Initial Operating Capability (IOC) date: 4/30/2022]
2. *The Security Plan Status Date:* In Process: [Initial Operating Capability (IOC) date: 4/30/2022]

3. *The Authorization Status:* In Process: [Initial Operating Capability (IOC) date: 4/30/2022]
4. *The Authorization Date:* In Process: [Initial Operating Capability (IOC) date: 4/30/2022]
5. *The Authorization Termination Date:* In Process: [Initial Operating Capability (IOC) date: 4/30/2022]
6. *The Risk Review Completion Date:* In Process: [Initial Operating Capability (IOC) date: 4/30/2022]
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH): MODERATE*

Section 9 – Technology Usage

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

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

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

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

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

The CCD utilizes cloud technology and a PaaS model and is hosted within the VA Enterprise Cloud (VAEC), AWS GovCloud, which is a FedRAMP approved environment.

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.

The CCD System resides is in the VA Enterprise Cloud (VAEC) which is a FedRAMP approved environment.

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.

The CCD System resides in the VA Enterprise Cloud (VAEC) which is a FedRAMP approved environment

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.

The CCD System resides in the VA Enterprise Cloud (VAEC) which is a FedRAMP approved environment, owned and operated by the VA Enterprise Cloud Service Office (ECSO).

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).

The CCD System resides in the VA Enterprise Cloud (VAEC) which is a FedRAMP approved environment and does not use RPA or AI.

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.

CHRISTIAN LOFTUS

Digitally signed by CHRISTIAN LOFTUS
Date: 2022.05.11 07:05:19 -04'00'

Privacy Officer, Christian Loftus

Karen A. McQuaid 321576

Digitally signed by Karen A. McQuaid 321576
Date: 2022.05.11 11:02:55 -05'00'

Information Systems Security Officer, Karen A. McQuaid

Michael F. Harry 1746757

Digitally signed by Michael F. Harry 1746757
Date: 2022.05.11 14:56:58 -04'00'

Information Systems Owner, Michael F. Harry

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).

Privacy, Policies, And Legal Information | Veterans Affairs

The VHA Notice of Privacy Practice (NOPP)
Patient Data Sharing Consent