Privacy Impact Assessment for the VA IT System called:

Integrated Veterans Care Centralized Data Repository (IVC CDR)

VA Office of Information Technology (OIT)

Integrated Veteran Care (IVC)

Date PIA submitted for review:

April 14, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Lynn A Olkowski	Lynn.Olkowski@va.gov	202-632-8405
Information System Security Officer (ISSO)	Crystal L White	crystal.white5@va.gov	813-972-2000 x7007
Information System Owner	Dena Liston	dena.liston@va.gov	304-886-7367

Abstract

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

Integrated Veterans Care Centralized Data Repository (IVC CDR) is a collection of datasets used to consolidate all Integrated Veterans Care into one repository. Datasets include the data from data collections/systems but not a collection of those systems. Those datasets are used for analytical and business improvement purposes.

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. The IT system name and the name of the program office that owns the IT system.

Integrated Veterans Care Centralized Data Repository (IVC CDR)
Integrated Veteran Care (IVC)

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

Integrated Veterans Care Centralized Data Repository (IVC CDR) is a collection of datasets used to consolidate all Integrated Veterans Care into one repository. Datasets include the data from data collections/systems but not a collection of those systems. Those datasets are used for analytical and business improvement purposes.

C. Indicate the ownership or control of the IT system or project.

VA Office of Information Technology (OIT)

2. Information Collection and Sharing

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

There are over 9 million Veterans enrolled in the VA whose information may be stored.

E. A general description of the information in the IT system and the purpose for collecting this information.

By serving as a consolidated repository of all Integrated Veterans Care, the datasets can be used for analytical and business improvement purposes.

F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.

Community Care Reimbursement System Database (CCRSDB) shares its data with IVC CDR.

CCRSDB is the database schema(s) for Community Care Reimbursement System (CCRS) that contains billing and reimbursement data.

G. 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.

The system is operated in the cloud and not at a physical site.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

SORN: 186VA10D - Community Care (CC) Provider Profile Management System (PPM)
SORN: 172VA10 - VHA Corporate Data Warehouse-VA
SORN: 205VA005OPA31C - Electronic Permission Access System (EPAS)-VA

Title 40 US Code § 1401 (3), Clinger-Cohen Act of 1996, which directs the development and maintenance of IT architectures by federal agencies to maximize benefits within the federal government.

U.S. Code Title 38, Section 527, VA is required to gather data for the purposes of planning and evaluating VA programs

I. 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?

Respective SORNs listed cover cloud use and storage.

SORN: 186VA10D - Community Care (CC) Provider Profile Management System (PPM)
Published 1/25/2021

SORN: 172VA10 - VHA Corporate Data Warehouse-VA
Published 12/22/2021

SORN: 205VA005OPA31C - Electronic Permission Access System (EPAS)-VA

D. System Changes

J. Whether the completion of this PIA will result in circumstances that require changes to business processes

No

K. Whether the completion of this PIA could potentially result in technology changes

No

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 Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ 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)

Additional Information Collected but Not Listed Above:

- Claim Information
- Family Relationship
- Disability Rating
- Guardian
- Employment Information
- Veteran Dependent Information
- Death Certificate Information
- VA User ID
- VA Email Address

PII Mapping of Components (Servers/Database)

IVC CDR consists of 1 key component (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by IVC CDR 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

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
Community Care Reimbursement System Database (CCRSDB)	YES	YES	Name, Integration Control Number, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers, Medical records, Claim Information, Race/Ethnicity,	To validate invoices submitted by contracted entities within the Community Care Network (CCN).	• Encryption at-rest. • Encryption in-transit. • Access Controls.

			Date of Death, Family Relationship, Disability Rating, Gender, Next of Kin, Guardian, Employment Information, Veteran Dependent Information, Death Certificate Information		

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?

IVC CDR receives data electronically and not from the record subjects.

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.

IVC CDR's purpose is to be a centralized data reposit in which the data stored in the IVC Information Technology system.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

IVC CDR creates information via analytical reports and dashboards.

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?

Yes, IVC CDR information is received via secure electronic transmission.

1.3b 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.

IVC CDR information is not collected on a form.

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.

IVC CDR is developed using the MuleSoft platform. MuleSoft has data integrity check capabilities that are configured to check data that is being loaded into IVC CDR. MuleSoft can be configured to perform a number of data integrity that includes deduplicate of records, ensure specific fields have data, and ensure the value or length data meet expected criteria.

1.4b 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.

IVC CDR only ingests information. It does not perform any accuracy checks.

1.5 What specific 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

IVC CDR is a new system and undergoing the ATO process to obtain FISMA authority to operate.

1.Title 40 US Code § 1401 (3), Clinger-Cohen Act of 1996, which directs the development and maintenance of IT architectures by federal agencies to maximize benefits within the federal government.

2.U.S. Code Title 38, Section 527, VA is required to gather data for the purposes of planning and evaluating VA programs

SORN: 186VA10D - Community Care (CC) Provider Profile Management System (PPM)

SORN: 172VA10 - VHA Corporate Data Warehouse-VA

SORN: 205VA005OPA31C - Electronic Permission Access System (EPAS)-VA

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

Principle of Purpose Specification: 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:

- Lack of data quality or safeguarding of integrity may lead to inaccurate analysis and reporting.

Mitigation:

- IVC CDR utilizes encrypted messaging as a data integrity mechanism during the data ingestion process to help ensure data integrity.

Section 2. Uses of the Information

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

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

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

IVC CDR serves as a consolidated repository of all Integrated Veterans Care, the data and datasets are used for conducting analysis towards business improvement purposes.

Name – Used a patient name
Social Security Number – Used as patient identifier
Date of Birth – Used to identify patient age and secondary identity validation
Personal Mailing Address – Used for patient mailing address
Health Insurance Beneficiary Numbers – Used as the patient beneficiary's health insurance number
Medical Records – Used as patient medical record information
Gender – Used to identify patient gender
Integrated Control Number (ICN) – Unique patient identifier, is assigned to each VA Corporate Data Warehouse (CDW) record used as a cross-indexed.
Next of Kin – Used to identify patient next of kin
Claim Information – Used to store patient claim information
Family Relationship – Used to identify patient relationship in family
Disability Rating – Used to store patient disability rating
Guardian – Used to identify patient guardian
Employment Information – Used to store patient employment information
Veteran Dependent Information – Used to store patient dependent information
Death Certificate Information – Used to store patient death certificate information
VA User ID – Used to store VA User ID
VA Email Address – Used for communicating with VA User via email

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 IVC CDR is the Mulesoft platform installed within the VAEC. The Mulesoft platform has built-in analytical capabilities for users to perform analytical reporting on the data collected.

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.

IVC CDR does not create new information but allows for data analytics on existing information collected.

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?

When data is copied into IVC CDR, this is performed using an encrypted connection using HTTPS/TLS with FIPS 140-2-compliant 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 within IVC CDR is safeguarded as sensitive data with encryption standards implemented for both data at rest and in transit. In addition, role-based access control (RBAC) is enforced with appropriate account management process to ensure appropriate need to know justification is in place.

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

IVC CDR is designed to have appropriate administrative, technical and physical security controls in place. As stated above, all data within IVC CDR is safeguarded as sensitive data with encryption standards implemented for both data at rest and in transit. In addition, role-based access control (RBAC) is enforced with appropriate account management process to ensure appropriate need to know justification is in place.

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?

Access requirements to IVC CDR which would include access to the stored PII is determined by the IVC CDR Business Owner. Currently this is Mr. Edward Ohrt. The determination of access includes business justification for access that identifies how Need-to-Know and Least-Privilege principles are met.

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

Access criteria, procedures, controls, and responsibilities are documented in the IVC CDR Access Control SOP.

2.4c Does access require manager approval?

Yes, a chain of manager approvals is required starting with the Employee/Contractor Supervisor approval to provide contracted support and the IVC CDR VA Project Manager approval to provision access to perform contracted support duties.

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

Yes, IVC CDR has audit log capabilities to track use of the system including access to PII.

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

The VA Information System Owner (ISO) is appointed to assure that safeguards for PII are in place and being enforced. An ISO Attestation memo is signed by the ISO attesting to this responsibility.

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
- Health Insurance Beneficiary Numbers
- Medical Records
- Gender
- Integrated Control Number (ICN)
- Next of Kin

Other Data Elements:

- Claim Information
- Family Relationship
- Disability Rating
- Guardian
- Employment Information
- Veteran Dependent Information
- Death Certificate Information
- VA User ID
- VA Email Address

3.2 How long is information retained?

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

IVC CDR data will be according to the source system. Currently the CCRS data has a 6 year retention.

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, Veterans Health Administration (VHA) RECORDS CONTROL SCHEDULE 10-1

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

Per Veterans Health Administration (VHA) RECORDS CONTROL SCHEDULE 10-1

Item Number: 1260.1

Records Description:
Care in Community: Care in the Community, Health and Medical Care Program records include but not limited to: Veteran and beneficiary claim and administrative records related to receiving health care services at VA expense outside VA facilities. A typical record file includes eligibility information, claim forms, medical records in support of claims and data concerning health care providers, services provided, amounts claimed and paid for health care services.

c. Electronic Records. (Master Files) Electronic records produced from scanned documents or records received electronically (optical disk, magnetic tape or other electronic medium).

Disposition Instructions: Temporary. Destroy 6 years after all individuals in the record become ineligible for program benefits.

Disposition Authority: N1-15-03-1, item 3

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.

All IVC CDR does not maintain paper records. If requested electronic data destruction is completed in accordance with VA Handbook 6500.1, Electronic Media Sanitization. Below is the IVC CDR purging procedure in accordance with the handbook:

Purging Procedures:

(1) Purging is the sanitization, or removal, of data from a system or storage device with the intent of the data not able to be reconstructed by laboratory techniques. For some media, clearing does not suffice for purging. However, for ATA hard disk drives manufactured after 2001 (over 15GB), the terms clearing and purging have converged. A laboratory attack involves a threat using advanced equipment, resources, and knowledge to conduct data recovery attempts on media outside its normal operating environment.

(2) Executing the Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. The sensitivity of the data stored on the computer and the feasibility of software purging should be weighed before degaussing hard drives. Degaussing of any hard drive assembly usually destroys the drive, as the firmware that manages the device is also destroyed. NIST

SP 800-88, Guidelines for Media Sanitization, includes a reference to the software, Secure Erase, from the University of California, San Diego (UCSD) Center for Magnetic Recording Research (CMRR) site and a link for downloading.

(3) Degaussing is exposing magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (low energy or high energy) of magnetic media they can purge and operate using either a strong permanent magnet or an electromagnetic coil. Degaussing is an effective method for purging damaged media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. In some circumstances, degaussing does not guarantee complete data destruction. For example, using under-strength degaussing equipment will not ensure complete data purging. Always ensure the appropriate degaussing equipment is matched with the media being degaussed. Proper degaussing will ensure insufficient magnetization left behind in a medium (referred to as data remanence) to reconstruct the data. Degaussing is not effective for purging non-magnetic media, such as optical media CDs or digital versatile discs (DVD) and these must be destroyed.

(4) VA approved degaussers are those which have been tested and approved by the National Security Agency (NSA). NSA publishes a list of evaluated degaussers, the Degausser Products List (DPL). A current copy of the DPL is available at www.nsa.gov. The introduction to the DPL explains how to determine the appropriate degausser for magnetic tape and magnetic disk media. Do not assume all of the degaussers listed are capable of erasing all formats of magnetic tape or magnetic disk media.
(5) Degaussing has risks which must be mitigated; incorrect usage of degaussing equipment can compromise data residing on storage media. For example, storage media removed before the degaussing cycle is complete will create data remanence on the storage media. Another risk involves using the wrong degausser for a specific media. Correctly labeling the coercivity of the media will help mitigate this risk. Use the NSA DPL for definitions and coercivity levels of magnetic tapes, magnetic disks, and approved degaussers.

(6) Degaussing equipment must be tested and certified periodically. Preventive maintenance must occur on a regular schedule to preclude mechanical or electrical problems. Some manufacturers have maintenance contracts and recommended maintenance schedules to ensure the integrity of the degaussing procedure. After installation, a degausser must be tested every 6 months for its first 2 years of operation and annually thereafter, as specified in the current NSA DPL. Verify with the manufacturer of the equipment if specific testing procedures are used. Test and diagnostic equipment used on devices with storage media can collect sensitive information; therefore, test and diagnostic devices must be purged after use to safeguard against this risk.

(7) Magnetic media stored for an extended period of time or under high temperature (exceeding 120 degrees Fahrenheit) becomes difficult to degauss. Each facility should have a media rotation process and is responsible for providing a stable environment for magnetic media storage. If purging media is not a reasonable sanitization method, magnetic media containing VA sensitive information must be destroyed.

(8) Ensuring labels are applied to magnetic tapes to identify the coercivity of the media upon initial use: Magnetic disk coercivities are identified by date of manufacture or date of purchase. Maintain a list of magnetic disk drive models, serial numbers, and purchase dates upon initial use. Strict

inventory controls should be in place to ensure magnetic tape and disk coercivities can be identified so the correct purge procedure is used for sanitization of the magnetic media.

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.

IVC CDR uses a Production-Test environment which contains a copy of production data that includes PII for testing purposes. As such, the Production-Test environment is configured with the same security control safeguards as the production environment.

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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:

<u>Privacy Risk:</u>
There is a risk with retaining data perpetually to ensuring ongoing confidentiality and assure its accuracy and integrity.

Mitigation:
IVC CDR adheres to the Principle of Data Quality and Integrity and complies retention schedules defined in the Veterans Health Administration (VHA) RECORDS CONTROL SCHEDULE 10-1. On a monthly basis IVC CDR will review records for disposal according to applicable schedule.

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.
vpl
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 infYHormation?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Health Administration (VHA) Program Integrity Tool (PIT)	Provide dataset to be consolidated with other Integrated Veterans Care datasets into	Name, Integration Control Number, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary	Drop zone, file transmission using Secure File Transfer Protocol (SFTP) over

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*
	one repository. Those datasets are used for analytical and business improvement purposes.	Numbers, Medical records, Claim Information, Race/Ethnicity, Date of Death, Family Relationship, Disability Rating, Gender, Next of Kin, Guardian, Employment Information, Veteran Dependent Information, Death Certificate Information	secured encryption and leveraging Identity Access Management (IAM) security accounts. Network connection over port 443 orchestrated by a Kafka service.
Veterans Health Administration (VHA) Community Care Referrals and Authorization System Assessing (CCRA)	Provide dataset to be consolidated with other Integrated Veterans Care datasets into one repository. Those datasets are used for analytical and business improvement purposes.	Name, Integration Control Number, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers, Medical records, Claim Information, Race/Ethnicity, Date of Death, Family Relationship, Disability Rating, Gender, Next of Kin, Guardian, Employment Information, Veteran Dependent Information, Death Certificate Information	Drop zone, file transmission using Secure File Transfer Protocol (SFTP) over secured encryption and leveraging Identity Access Management (IAM) security accounts. Network connection over port 443 orchestrated by a Kafka service.
Veterans Health Administration (VHA) Electronic Data Interchange (EDI) - General	Provide dataset to be consolidated with other Integrated Veterans Care datasets into one repository. Those datasets are used for analytical and business improvement purposes.	Name, Integration Control Number, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers, Medical records, Claim Information, Race/Ethnicity, Date of Death, Family Relationship, Disability Rating, Gender, Next of Kin, Guardian, Employment Information, Veteran Dependent Information, Death Certificate Information	Drop zone, file transmission using SFTP over secured encryption and leveraging IAM
Veterans Health Administration	Provide dataset to be consolidated	Name, Integration Control Number, Social Security	Drop zone, file transmission using

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*
(VHA) Provider Profile Management System (PPMS) Assessing	with other Integrated Veterans Care datasets into one repository. Those datasets are used for analytical and business improvement purposes.	Number, Date of Birth, Address, Zip Code	SFTP over secured encryption and leveraging IAM security accounts. PPMS is hosted in VAEC Visionary Artistry Magazine (VAMAG). Network connection over port 443 orchestrated by a Kafka service
Veterans Health Administration (VHA) Financial Management System	Provide dataset to be consolidated with other Integrated Veterans Care datasets into one repository. Those datasets are used for analytical and business improvement purposes.	Name, Social Security Number, Mailing address, Email address, Telephone number, Emergency contact information, Financial account information, Banking information, Disabilities, Criminal record information, Service information, Veterans preference information, Student loans, Education background, Savings plan information, Benefits information, Taxpayer identification number (TIN), Credit card number, Claim number, Claims for non-VA care, Provider name, Dates service rendered, Description of service (may include diagnosis), Duplicate payment information, Control number	Drop zone, file transmission using SFTP over secured encryption and leveraging IAM security accounts. Network connection over port 443 orchestrated by a Kafka service.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (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:
The risk associated with internal sharing is the unauthorized or unintended disclosure of information via reports generated from IVC CDR.

Mitigation:
IVC CDR maintains access control to restrict access only to authorized users with appropriate role-based access. All access is granted based on management approval and need-to-know justification.

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	***List the purpose of***	***List the specific PII/PHI data elements that are processed***	***List the legal***	***List the method of***

or IT System information is shared/received with	*information being shared / received / transmitted with the specified program office or IT system*	*(shared/received/transmitted) with the Program or IT system*	*authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*transmission and the measures in place to secure data*
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk:
There is no external data sharing between IVC CDR and any other entities outside of the VA. In regards to unknow external malicious threats, IVC CDR resides within the VAEC environment which monitors the network for suspicious activity and intrusion detection. In addition, IVC CDR maintains audit logs of activity that is monitored for suspicious activity.

Mitigation:
N/A

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 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.

IVC CDR does not collect information directly from individuals. All information is provided by other VA systems.

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

IVC CDR does not collect information directly from individuals. However, per VHA DIRECTIVE 1605.01, VA may not collect or maintain information about individuals that is retrieved by a personal identifier until proper notifications are given to Congress and the Office of Management and Budget (OMB), and a notice is published in the Federal Register as required by the Privacy Act. The VA Notice of Privacy Practices can be found at the following website: https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=10127

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.

IVC CDR does not collect information directly from individuals. However, per VHA DIRECTIVE 1605.01, VA may not collect or maintain information about individuals that is retrieved by a personal identifier until proper notifications are given to Congress and the Office of Management and Budget (OMB), and a notice is published in the Federal Register as required by the Privacy Act. The VA Notice of Privacy Practices can be found at the following website: https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=10127

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.

IVC CDR does not collect information directly from individuals. However, per VHA DIRECTIVE 1605.01, VA may not collect or maintain information about individuals that is retrieved by a personal identifier until proper notifications are given to Congress and the Office of Management and Budget (OMB), and a notice is published in the Federal Register as required by the Privacy Act. The VA Notice of Privacy Practices can be found at the following website: https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=10127

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.

IVC CDR does not collect information directly from individuals. However, per VHA DIRECTIVE 1605.01, VA may not collect or maintain information about individuals that is retrieved by a personal identifier until proper notifications are given to Congress and the Office of Management and Budget (OMB), and a notice is published in the Federal Register as required by the Privacy Act. The VA Notice of Privacy Practices can be found at the following website: https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=10127

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:
IVC CDR does not collect information directly from individuals.
Mitigation:
Per VHA DIRECTIVE 1605.01, VA may not collect or maintain information about individuals that is retrieved by a personal identifier until proper notifications are given to Congress and the Office of Management and Budget (OMB), and a notice is published in the Federal Register as required by the Privacy Act. The VA Notice of Privacy Practices can be found at the following website: https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=10127.

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.***

IVC CDR information is aggregated from multiple VA systems. An individual who wishes to gain information regarding their data would submit their request to the VA according to the instructions of the source VA system that gathered their information. Should an individual request require information on their data maintained in IVC CDR, such a request would come from the source VA system which obtained the request.

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).

IVC CDR is 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 following statement is standard VA language for SORN systems:
An individual who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or wants to review the contents of such record, should submit a written request or apply in person to the last VA health care facility where care was rendered. Addresses of VA health care facilities may be found in VA Appendix 1 of the Biennial Publication of Privacy Act Issuances. All inquiries must reasonably describe the portion of the medical record involved and the place and approximate date that medical care was provided. Inquiries should include the patient's full name, Social Security number, and return address.

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.

SORN NOTIFICATION PROCEDURE: An individual who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or wants to review the contents of such record, should submit a written request or apply in person to the last VA health care facility where care was rendered. Addresses of VA health care facilities may be found in VA Appendix 1 of the Biennial Publication of Privacy Act Issuances. All inquiries must reasonably describe the portion of the medical record involved and the place and approximate date that medical

care was provided. Inquiries should include the patient's full name, Social Security number, and return address.

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 informed via the respective SORNs of data sources from which IVC CDR receives data of procedures to correct their information. The following are those SORNs:

- SORN: 186VA10D - Community Care (CC) Provider Profile Management System (PPM)
- SORN: 172VA10 - VHA Corporate Data Warehouse-VA
- SORN: 205VA005OPA31C - Electronic Permission Access System (EPAS)-VA

SORN NOTIFICATION PROCEDURE: An individual who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or wants to review the contents of such record, should submit a written request or apply in person to the last VA health care facility where care was rendered. Addresses of VA health care facilities may be found in VA Appendix 1 of the Biennial Publication of Privacy Act Issuances. All inquiries must reasonably describe the portion of the medical record involved and the place and approximate date that medical care was provided. Inquiries should include the patient's full name, Social Security number, and return address.

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.

Individuals should follow guidance provided in a VA system's SORN regarding redress for access to their information. An individual who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or wants to review the contents of such record, should submit a written request or apply in person to the last VA health care facility where care was rendered. Addresses of VA health care facilities may be found in VA Appendix 1 of the Biennial Publication of Privacy Act Issuances. All inquiries must reasonably describe the portion of the medical record involved and the place and approximate date that medical care was provided. Inquiries should include the patient's full name, Social Security number, and return address

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:
There is a risk that an individual is not aware that their data being stored in IVC CDR and no process by which they can make such an inquiry.

Mitigation:
A formal VA procedure exists where individuals can inquire about the data being stored in VA Systems. Individuals are informed via a SORN of procedures to correct their information. SORN NOTIFICATION PROCEDURE: An individual who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or wants to review the contents of such record, should submit a written request or apply in person to the last VA health care facility where care was rendered. Addresses of VA health care facilities may be found in VA Appendix 1 of the Biennial Publication of Privacy Act Issuances. All inquiries must reasonably describe the portion of the medical record involved and the place and approximate date that medical care was provided. Inquiries should include the patient's full name, Social Security number, and return address.
.

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.

IVC CDR maintains an Access Control Standard Operating Procedures (SOP) document that articulates the process and controls in place for gaining authorization and access to IVC CDR.

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?

No users from other agencies outside of the VA have access to IVC CDR.

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.

General user access to IVC CDR is read-only. Privileged user access that would allow a user to conduct analytical functions with limited edit capabilities. Finally administrative access is for administrators of IVC CDR with full access to IVC CDR functions and data.

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.

Yes, VA contractors responsible for the program management and technical administration of IVC CDR have access to the data which contains PII. All contractors must have an NDA and Rules of Behavior agreements in place prior to being granted access to IVC CDR. VA Contractors are defined to be non-VA employed resources contracted to the VA to perform contracted services. These VA contractors are required to sign an NDA.

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 IVC CDR users must comply with annual VA Cybersecurity Awareness training and VA Privacy Awareness training: VA Privacy and Information Security Awareness and Rules of Behavior (WBT) VA TMS #10176

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

8.4a If Yes, provide:

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

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.***

No, IVC CDR is a new system and currently going through the VA Risk Management Framework (VA RMF) process to obtain an Authority to Operate (ATO). A tentative IOC date is April 2023.

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, IVC CDR with using the VA Enterprise Cloud (VAEC).

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.*

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.

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.

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).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**

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

Signature of Responsible Officials

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

Lynn A Olkowski

Digitally signed by Lynn A Olkowski
Date: 2023.04.26 07:41:29 -05'00'

Privacy Officer, Lynn A Olkowski

CRYSTAL L. WHITE 134339

Digitally signed by CRYSTAL L. WHITE 134339
Date: 2023.04.19 16:12:45 -04'00'

Information System Security Officer, Crystal L White

DENA LISTON

Digitally signed by DENA LISTON
Date: 2023.04.25 19:15:06 -04'00'

Information System Owner Dena Liston,

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).

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

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