Privacy Impact Assessment for the VA IT System called:

Community Care Clinical and BI Solution - Enterprise Reporting System Assessing Veterans Health Administration Office of Integrated Veteran Care (IVC)

Date PIA submitted for review:

08/04/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Michael Hartmann	Michael.Hartmann@va.gov	303-780-4753
Information System Security Officer (ISSO)	Peter Tadalan	PeterPol.Tadalan@va.gov	(916) 212-4227
Information System Owner	Chris Brown	Christopher.brown1@va.gov	202-270-1432

Abstract

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

The Community Care Clinical and BI Solution - Enterprise Reporting System Assessing also known as Enterprise Program Reporting System (EPRS) is the VA's quintessential source for Community Care Network's reporting and analytical tools. The solution provides:

A.) aggregate and detail patient episode of care data for each network contract

B.) a view to operational aspects of the Veterans Affairs Health Administration (VHA) Office of Community Care (OCC) associated with contract implementation, management, and maintenance

C.) assists in examining network contract activity and performance and addresses the measurements of the Contract QASP (Quality Assurance Surveillance Plan)

D.) provides stakeholders the ability to drill down on specific data and produce metrics which could result in identifying opportunities for improved community care business processes, performance and timeliness and acts as facilitator of data to other downstream data consumers. Performance Improvement & Reporting (PI&R) Informatics uses an internal VHA Intranet based web page with approximately 40 to 50 reports viewable for individuals with access via VHA National Data Systems under VHA Office of Information and Technology (OI&T). When the program is fully implemented, the user population is estimated at MAh7,000 users. Users will consist of internal VHA staff only.

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 VHA/IVC Community Care Clinical and BI Solution - Enterprise Reporting System Assessing also known as Enterprise Program Reporting System (EPRS) is the VA's quintessential source for Community Care Network's reporting and analytical tools.
EPRS is not a FY22 CCC & BI EPRS - PIA Draft regional General Support System (GSS), Veterans' Health Information Systems and Technology Architecture (VistA) VistA, or Local Area Network (LAN).

EPRS is a web-based reporting system that provides –

- aggregate and detail patient episode of care data for each network contract
- a view to operational aspects of the VHA OCC associated with contract implementation, management and maintenance
- assists in examining network contract activity and performance and addresses the measurements of the Contract Quality Assurance Surveillance Plan (QASP)
- provides stakeholders the ability to drill down on specific data and produce metrics which could result in identifying opportunities for improved community care business processes, performance and timeliness and act as facilitator of data to other downstream data consumers

- utilizes SharePoint for user data entry to augment other report sources
- integrates with EDI gateway to process claims (X12) transactions to include with reports
- processes CCN contractor deliverables to gather information regarding health care delivery

EPRS provides a web application that runs on Microsoft Power BI (Business Intelligence) in a given user's browser. EPRS infrastructure is centrally hosted on the Microsoft Azure GovCloud (MAG). The current System of Records Notice (SORN) are applicable and will not need to be updated or modified for this system or collection. The applicable legal authority falls under SORN: 23VA10NB3, 79VA10: Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111,501, 1151 1703, 1705, 1710, 1712, 1717,1720, 1721, 1724, 1725, 1727, 1728,1741 – 1743, 1781, 1786, 1787, 3102,5701 (b) (6) (g) (2) (g) (4) (c) (1), 5724, 7105,7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014 and SORN 54VA10NB3: Title 38, United States Code, sections 501(a), 501(b), 1703, 1720G, 1724, 1725, 1728, 1781, 1787, 1802, 1803, 1812, 1813, 1821, Public Law 103–446 section 107 and Public Law 111–163 section 101. EPRS is hosted within the Azure FedRAMP HIGH Veterans Affairs Enterprise Cloud (VAEC). The virtual machines, operating systems, as well as applications are secured and then validated by both the VAEC cloud team and the VA Software Assurance organization and tracked within the programs ATO. All the EPRS data at rest is encrypted using Federal Information Processing Standards (FIPS) 140-2, all the data transfer inside VA secure data domain by following Corporate Data Warehouse (CDW) and National Data Systems (NDS) guidance. Completion of this PIA would not affect any technology or business process changes. Ownership data rights stay within the VA, there is no external sharing. Magnitude of harm if the privacy related data in a case of disclosure due to the volume of users and the data collection the harm would be extensive. In the first year, EPRS audience is estimated at 5000 users. When the program is fully implemented, the user population may reach an estimated 7,000 users.

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)

- City
- State
- Zip Code
- National Provider Identifier (NPI)
- Member ID

PII Mapping of Components

EPRS consists of four key components. Each component has been analyzed to determine if any data elements of that component collect PII. The type of PII collected by EPRS and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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.

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
LSV CBOPC_EPRS SPV	Yes	Yes	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Current Medications, Previous Medical Records, Tax Identification Number, Member ID	Source for CCN's reporting and analytical tools	Secure VA Network (HTTPS or TLS), Azure Express Route (AER) (encrypted), VAEC Trusted Internet Connections (TIC)
CDWWork	Yes	Yes	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Current Medications, Previous Medical Records, Tax Identification Number, Member ID	Source for CCN's reporting and analytical tools	Secure VA Network (HTTPS or TLS), Azure Express Route (AER) (encrypted), VAEC Trusted Internet Connections (TIC)

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
E_REPOS	Yes	Yes	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Financial Account Information, Certificate/License numbers, Health Insurance Beneficiary Numbers, Current Medications, Previous Medical Records, Tax Identification Number, Medical Record Number, Member ID	Source for CCN's reporting and analytical tools	Secure VA Network (HTTPS or TLS), Azure Express Route (AER) (encrypted), VAEC Trusted Internet Connections (TIC)
CCRSDB_Prod	Yes	Yes	Claims, Referrals, Payments, Social Security Numbers	Source for CCN's reporting and analytical tools	Secure VA Network (HTTPS or TLS), Azure Express Route (AER) (encrypted), VAEC Trusted Internet Connections (TIC)

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.

EPRS will source data from the CDW and external CCN Contractors and will store the retrieved data for further processing and reporting. In addition, through the EPRS SharePoint, users are able to enter data related to contract variances.

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 technology 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.

EPRS will gather data from the CDW and external CCN Contractors. Additionally, users are able to enter data related to contract variances through the EPRS SharePoint.

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.

EPRS is dependent on data consistency checks performed by the CDW and third-party contractors that it relies on for data. However, additional data validation checks will be designed to ensure that the data being pulled from various authoritative systems is an accurate representation. However, since EPRS is not an authoritative source but instead a downstream consumer of data from other authoritative systems, EPRS bears no responsibility for making sure that authoritative sources have their data correct. However, reports could be developed to assist the field in identifying problems with data content in authoritative sources that the field can then go to the authoritative sources to correct.

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 applicable legal authority falls under SORNs: 23VA10NB3, 79VA10: Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111,501, 1151 1703, 1705, 1710, 1712, 1717,1720, 1721, 1724, 1725, 1727, 1728,1741–1743, 1781, 1786, 1787, 3102, 5701 (b) (6) (g) (2) (g) (4) (c) (1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014 and SORN 54VA10NB3: Title 38, United States Code, sections 501 (a), 501 (b), 1703, 1720G, 1724, 1725, 1728, 1781, 1787, 1802, 1803, 1812, 1813, 1821, Public Law 103–446 section 107 and Public Law 111–163 section 101.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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:

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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: Personally Identifiable Information (PII) of a Veteran/Beneficiary may not be accurate, complete, and current in the EPRS System.

Mitigation: EPRS relies on the source (feeder) systems to ensure that personally identifiable information is accurate, complete, and current. The following policies and procedures in the VA ensure that any PII collected and maintained by VA is accurate, relevant, timely, and complete for the purpose for which it is to be used:

- requires a Veteran or an authorized representative to validate PII during the collection process
- when required, requests Veteran or an authorized representative to revalidate that PII collected is still accurate
- confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information;
- collects PII directly from the individual to the greatest extent practicable
- checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems; and
- issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

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.

- Name: for beneficiary identification
- Social Security Number (SSN): for beneficiary identity and as a file number for the beneficiary
- Date of Birth: for beneficiary identification
- Personal Mailing Address: to verify the correct address
- Personal Phone Number(s): to verify the correct phone number
- Personal Email Address: to run reports for use of community care
- Emergency Contact Info: to run reports for use of community care
- Financial Account Info: to run reports for use of community care
- Certificate/License numbers: to run reports for use of community care

- Health Insurance Beneficiary Numbers: to run reports for use of community care
- Current Medications: to run reports for use of community care
- Previous Medical Records: to run reports for use of community care
- Tax Identification Number (TIN): to run reports for use of community care
- Medical Record Number: to run reports for use of community care
- Member ID: to run reports for use of community care
- Contractor Name: to run reports for use of community care
- Contractor Personal Address: to run reports for use of community care
- Contractors Personal Telephone Number(s): to run reports for use of community care
- The National Provider Identifier (NPI) is a Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Standard. The NPI is a unique identification number for covered health care providers: to run reports for use of community care.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

EPRS reports operational, programmatic and finance (revenue) data related to the CCN Contract to the IVC Business Line. These reports are used for Deputy Under Secretary for Health, Freedom of Information Act requests and provide the following information:

- aggregate and detail patient episode of care data for each network contract
- a view to operational aspects of the VHA OCC associated with contract implementation, management and maintenance
- assists in examining network contract activity and performance and addresses the measurements of the Contract QASP (Quality Assurance Surveillance Plan)
- stakeholders the ability to drill down on specific data and produce metrics which could result in identifying opportunities for improved community care business processes, performance and timeliness and acts as facilitator of data to other downstream data consumers

2.3 How is the information in the system secured?

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

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

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

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

The information in the EPRS web-based application is secured by encrypting data in transit and at rest.

To transmit data securely, data in transit is encrypted using FIPS-140-2 encryption using TLS v1.2. To the extent possible, data in transit is passed between services inside of the Virtual Network (VNET) within MAG cloud.

To hold data securely, data at rest is stored in an encrypted Azure Virtual Machine Data Disk. Azure SQL Database (PaaS) is encrypted by default from MAG cloud.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

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

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

<u>Principle of Use Limitation:</u> 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.

EPRS reports are created using Power BI, a business analytics service by Microsoft. Role-based security is implemented in the application to ensure that the reports are only accessible to the users through the secure Power BI interface, and they cannot be accessed directly. PII/PHI/SPI is protected in the application and only presented to users who are identified as having access to

PII/PHI/SPI. Reports are designed to conditionally show or hide PII/PHI/SPI in the chance that a user happens to accidentally be given a link to a report that the user isn't permitted to access. Auditing is performed of the report(s) the user selects.

Access to EPRS is possible only by an EPRS administrator granting access. Access is granted on a need-to-know basis. VA staff must complete the Access Request Form, which must be signed by staff (requester) and employee's supervisor for approval. The local Office of Information and Technology (OIT) will verify staff completed Privacy, Cyber Security Training, and Signed Rules of Behavior by signing the Access Request Form. This form will be sent to a designated mail group. The OIT will sign the Access Request Form, only at this point access will be granted by the administrators.

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 (SSN)
- Date of Birth
- Personal Mailing Address
- Personal Phone Number
- Personal Email Address
- Emergency Contact Info
- Financial Account Info
- Health Insurance Beneficiary Numbers
- Certificate/License numbers
- Current Medications
- Previous Medical Records
- Tax Identification Number (TIN)
- Medical Record Number
- Contractor Name
- Contractor Personal Address
- Contractor Personal Telephone Number(s)
- National Provider Identifier (NPI)

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.

Electronic Records (Master Files). Electronic records produced form scanned documents or records received electronically (optical disk, magnetic tape or another electronic medium). Temporary; destroy 6 years after all individuals in the record become ineligible for program benefits. (N1-15-03-1, item 3).

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.
This question is related to privacy control DM-2, Data Retention and Disposal.

Yes, VHA Records Control Schedule (RCS 10-1)
https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf

3.4 What are the procedures for the elimination of SPI?

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

The EPRS database will be deleted after decommissioning, following the Records Control Schedule (RCS 10-1).

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

Data in this system is not used for research, testing or training.

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

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

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

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

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

<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> PII and SPI data breach opportunity increases the longer the information is retained.

<u>Mitigation:</u> To combat the risk of PII and SPI being breached, the EPRS system will follow RCS 10-1, all data is physically destroyed 6 years after all individuals in the record become ineligible for program benefits.

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***
Corporate Data Warehouse (CDW)	EPRS is pulling the IT System data to organize the data into one centralized location/model for reporting	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Current Medications, Previous Medical Records, Tax Identification Number, Member ID	Secure VA Network (HTTPS or TLS) VAEC Trusted Internet Connections (TIC) Azure Express Route (AER) (encrypted)

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***
HealthShare Electronic Data Interchange (EDI)	Claim/Payment/Coordination of Benefits (EDI 835 and 837) data obtained from CCN Contractors is sent to HealthShare EDI for further processing. HealthShare EDI pulls the data, parses it and sends the results back to EPRS.	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Financial Account Information, Certificate/License numbers, Health Insurance Beneficiary Numbers, Current Medications, Previous Medical Records, Tax Identification Number, Medical Record Number, Member ID	Secure VA Network (HTTPS or TLS) VAEC Trusted Internet Connections (TIC) Azure Express Route (AER) (encrypted)
Active Directory Service Accounts (AD)	EPRS is pulling data from VA's Active Directory for Authentication and Authorization	VA Contractors: Name, Personal Mailing Address, Personal Phone Number(s)	Secure VA Network (HTTPS or TLS)
Community Care Reimbursement System (CCRS)	EPRS is pulling data from Community Care Reimbursement System (CCRS) for claims, referrals, payments, and social security numbers.	Claims, Referrals, Payments, Social Security Numbers	Secure VA Network (HTTPS or TLS) VAEC Trusted Internet Connections (TIC) Azure Express Route (AER) (encrypted)

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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

Follow the format below:

Privacy Risk: If access to the EPRS System is not monitored, there may be unauthorized use or disclosure within individuals who are not authorized to view the data.

Mitigation: The EPRS Project Team routinely monitors, tracks, and logs the organizational use of EPRS data as a preventive measure. VA personnel will be trained on the authorized uses of EPRS information as well as consequences of unauthorized use or sharing of PII to minimize the risk. In the event of a violation of policy, the Privacy Office will be notified immediately, and corrective action will be taken as deemed necessary and may involve temporary or permanent deactivation of the end user account in question.

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***
Optum	Organizing data into one centralized location for reporting operational, programmatic and finance (revenue) data related to the CCN Contract	Veterans and/or Dependent Data: Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Financial Account Info, Certificate/License numbers, Health Insurance Beneficiary Numbers, Current Medications, Previous Medical Records, Tax Identification Number, Medical Record Number, Member ID	Contract	TLS, SFTP, Azure Express Route (encrypted)
TriWest Healthcare Alliance	Organizing data into one centralized location for reporting operational, programmatic and finance (revenue) data related to the CCN Contract	Veterans and/or Dependent Data: Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Financial Account Info, Certificate/License numbers, Health Insurance Beneficiary Numbers, Current Medications, Previous Medical Records, Tax Identification Number, Medical Record Number, Member ID	Contract	TLS, SFTP, Azure Express Route (encrypted)

The Contracting Officer Representative (COR) is responsible for ensuring that all contractors who are working on OCC projects have signed any necessary contractual requirements governing access and handling of Veteran data. The EPRS Project Team is required to ensure that all contractors interfacing with EPRS data are adhering to VA policies and OMB Memorandum M-06-15 and OMB Memorandum M-06-16.

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: A Privacy Risk may arise if any EPRS data is accessed by unauthorized personnel outside the VA.

Mitigation: All EPRS application users must be VA cleared. No access is granted to non-VA users including contractors or any external departments. All access is routinely monitored, tracked, and logged. An Incident Response Plan (IRP) that describes the procedures and protocols for reporting and handling of information security incidents as required by the policies and laws of the U.S. Federal Government and the U.S. Department of Veterans Affairs has been formulated for EPRS.

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.

PII is collected on VA Form 1010EZ, OMB number: OMB Approved No. 2900-0091
VHA Privacy Notice: https://www.oprm.va.gov/privacy/about_privacy.aspx
VHA HANDBOOK 1605.04, Notice of Privacy Practices
VHA Directive 1605.01 D (2016-08-31) Privacy and Release of Information
VA Privacy Impact Assessment: https://www.oprm.va.gov/privacy/pia.aspx

VHA OCC CHAMPVA Guide:
https://www.va.gov/COMMUNITYCARE/docs/pubfiles/programguides/champva_guide.pdf

VHA Systems of Records Notice:
23VA10NB3: Non-VA Care (Fee) Records (Published on July 30, 2015)
54VA10NB3: Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files --VA (Published on March 3, 2015)

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

VHA Directive 1605.01 'Privacy and Release Information' lists the rights of beneficiaries to request the VHA to restrict the use and/or disclosures of individually-identifiable health information to carry out treatment, payment, or health care operations. Beneficiaries have the right to refuse to disclose their SSNs to the VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (please refer to the 38 Code of Federal Regulations CFR 1.575(a)).

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

VHA Directive 1605.01, Privacy and Release Information list the rights of Beneficiaries to request that the VHA restrict the uses and/or disclosures of individually-identifiable health information to carry out treatment, payment, or health care operations.

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 a Privacy Notice is not provided to the subjects of the record, the public would not be aware of the information collected, used, retained and disclosed by the System.

Mitigation: The VA mitigates this risk by ensuring that this PIA, which serves as notice that EPRS exists, what information it contains, and the procedures in managing the information is available online per the requirements of the eGovernment Act of 2002, Publication. L. 107–347 §208 (b) (1) (B) (iii). Veterans receive a VHA Privacy Notice at the point of service and Beneficiaries are given a VHA Privacy Notice through the ChampVA Guide Book.

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.

VHA Directive 1605.01: Privacy and Release Information states the rights of Beneficiaries to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access to data must be delivered to, and reviewed by, the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

CDW is the authoritative source for all internal data. In the event that data stored in the authoritative sources are erroneous, the EPRS personnel can take a note, but cannot correct inaccurate or erroneous information.

However, if a correction is requested by a Beneficiary or Provider, then such a request must be in writing and it must adequately describe the specific information that the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned system of records, and the facility Privacy Officer, or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. VHA Directive 1605.01, Appendix D: Privacy and Release Information, Section 5 lists the rights of Beneficiaries to request that the VHA restrict the uses and/or disclosures of individually-identifiable health information to carry out treatment, payment, or health care operations.

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.

The authoritative source for the data is CDW. In the event that data stored in the authoritative sources are erroneous, the EPRS personnel can take a note, but cannot correct inaccurate or erroneous information.

However, if a correction is requested by a Beneficiary or Provider, then such a request must be in writing and it must adequately describe the specific information that the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned system of records, and the facility Privacy Officer, or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. VHA Directive 1605.01, Appendix D: Privacy and Release Information, Section 5 lists the rights of Beneficiaries to request that the VHA restrict the uses and/or disclosures of individually-identifiable health information to carry out treatment, payment, or health care operations.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

If the Veteran/Beneficiary discovers that incorrect information was provided during intake, they simply follow the same contact procedures in section 7.3 (also re-stated below), and state that the documentation they are now providing supersedes those previously provided.

If a Veteran/Beneficiary discovers that incorrect information was provided during the intake process, the request must be in writing and adequately describe the specific information the Veteran/Beneficiary believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: The EPRS System denies a Veteran/Beneficiary direct access, redress and correction of their record maintained in the System. This may result in inaccurate Veteran/ Beneficiary information making its way into the system.

Mitigation: A veteran/beneficiary who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or who wants to review the contents of such a record, should submit a written request or apply in person to the VA health care facility (or directly to the VHA) where care was rendered. Inquiries should include the patient's full name, SSN, 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?

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 EPRS is possible only by an EPRS administrator granting access. Access is granted on a need-to-know basis. VA staff must complete the Access Request Form, which must be signed by staff (requester) and employee's supervisor for approval. The local OIT will verify staff completed Privacy, Cyber Security Training, and Signed Rules of Behavior by signing the Access Request Form. This form will be sent to a designated mail group. The OIT will sign the Access Request Form, only at this point access will be granted by the administrators.

All EPRS application users must be VA cleared users from other agencies (non-VA personnel) are not permitted to use the system. All user accounts allow read only access to data. A role-based access control (RBAC) security approach is used to limit users only to the information needed to do their job and prevent them from accessing information that doesn't pertain to them.

There are a variety of user roles which will access the system, ranging from administrators, supervisors, and Community Care Stakeholders (consume reports). The EPRS user profiles are shown in the table below based upon current requirements.

Role	Function
User/Stakeholder	View Reports (Read-Only)
Community Care Stakeholder	Reports/Data Entry
Community Care Field Assistant	View Reports (Read-Only)
CCN Administration Stakeholder	View Reports (Read-Only)
CC CRT Stakeholder	View Reports (Read-Only)

EPRS Development Contractors create and maintain administrative accounts with advanced levels of access to support their duties. The administrative accounts have been verified by the project ISO through an access request process and only those individuals who have taken the required training and agreed to the Rules of Behavior (RoB) are granted administrative access to the EPRS environments.

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.

The Contracting Officer Representative (COR) is responsible for ensuring that all contractors who are working on the EPRS project have signed Non-Disclosure Agreements and necessary contractual requirements governing access and handling of Veteran data. The EPRS Project Team is required to ensure that all contractors interfacing with EPRS data are adhering to VA policies and OMB Memorandum M-06-15 and OMB Memorandum M-06-16. According to OMB Memorandum M-17-15, OMB Memorandum M-06-16 is rescinded and captured within other policies and NIST standards (https://policy.cio.gov/rescissions-identity-management/). Necessary roles and responsibilities have been established to restrict certain users to different access levels.

- Contractors developing the information system do not have direct access to the EPRS database. However, to support development and testing efforts, contractors have access to EPRS data via Web Services used by various other programs/projects which access EPRS data.
- Contractors maintaining the information system have elevated access to the EPRS database in order to support various development and maintenance activities.

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.

Personnel who will be accessing the system must read and acknowledge their receipt and acceptance of the VA Information Security RoB prior to gaining access to the EPRS system. The rules are included as part of the security awareness training that all personnel must complete via the VA's Talent Management System (TMS). After the MbM user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. This training includes, but is not limited to, the following TMS Courses:

- VA 10176: Privacy and Info Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training
- VA 3812493: Annual Government Ethics Role-based Training includes but is not limited to and based on the role of the user.
- VA 1016925: Information Assurance for Software Developers IT Software Developers
- VA 3193: Information Security for CIOs Executives, Senior Managers, CIOs and CFOs
- VA 1357084: Information Security Role-Based Training for Data Managers
- VA 64899: Information Security Role-Based Training for IT Project Managers
- VA 3197: Information Security Role-Based Training for IT Specialists
- VA 1357083: Information Security Role-Based Training for Network Administrators
- VA 1357076: Information Security Role-Based Training for System Administrators
- VA 3867207: Information Security Role-Based Training for System Owners

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

If Yes, provide:

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

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

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

The Security Plan Status has been completed and signed on 14 December 2021. On January 27th, 2022, Enterprise Reporting System (EPRS) General Support System (GSS) was awarded a 3 Year ATO by Authorizing Official Reginald Cummings. Authorization Termination Date (ATD) is January 26th, 2025. The Risk Review Completion Date is 19 January 2022.The FIPS 199 classification for EPRS is 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 EPRS web-based application system is hosted by the VA Enterprise Cloud (VAEC) and is identified as an IaaS.

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.

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**
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 they provided in this Privacy Impact Assessment is true and accurate.

Michael D Hartmann 1612370

Digitally signed by Michael D Hartmann 1612370
Date: 2022.08.16 08:05:14 -06'00'

Privacy Officer, Michael Hartmann

PETER POL G. TADALAN 637890

Digitally signed by PETER POL G. TADALAN 637890
Date: 2022.08.17 05:54:31 +08'00'

Information System Security Officer, Peter Tadalan

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2022.08.15 16:21:56 -05'00'

Information System Owner, Chris Brown

APPENDIX A

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):

- 23VA10NB3: Non-VA Care (Fee) Records (Published on July 30, 2015)
- 54VA10NB3: Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files --VA (Published on March 3, 2015)
- Department of Veterans Affairs Veterans Health Administration NOTICE OF PRIVACY PRACTICES