Privacy Impact Assessment for the VA IT System called:

Community Care Clinical and BI Solution-Enterprise Reporting System Assessing (EPRS)

Veterans' Health Administration

Office of Integrated Veteran Care (IVC)

eMASS ID # 759

Date PIA submitted for review:

1/31/2025

System Contacts:

System Contacts

Title	Name	E-mail	Phone Number
Privacy Officer	Eller Pamintuan	Eller.Pamintuan@va.gov	303-331-7512
Information System Security Officer (ISSO)	Jeffrey Skaggs	Jeff.Skaggs@va.gov	559-307-4308
Information System Owner	Tony Sines	Tony.Sines@va.gov	316-249-8510

Abstract

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

Community Care Clinical and BI Solution – Enterprise Reporting System Assessing (EPRS) (eMASS ID# 759) enables Veterans Health Administration (VHA) Office of Integrated Veteran Care (IVC) and VHA Leadership to monitor the Veteran's journey through the community care processes, supporting contractor accountability and informing program improvement efforts through various reporting metrics. EPRS collects detailed data for reports pulled from Corporate Data Warehouse (CDW) and other data systems including data provided by Community Care Network via Data Access Services (DAS). The EPRS system collects data for all Community Care level reporting for VHA Community Care Program (CCP). Data from many CCP systems and the Community Care Network (CCN) contractors is imported into EPRS daily. The front-end user interface for this system is Microsoft Power Platform Power Application.

Overview

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

1 General Description

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

EPRS is the VA's quintessential source for Community Care Network's reporting and analytical tools.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

Community Care Clinical and BI Solution – Enterprise Reporting System Assessing, also known as Enterprise Program Reporting System (EPRS), is owned by the Office of Integrated Veteran Care (IVC).

2. Information Collection and Sharing

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

The expected number of individuals would be in the millions. The typical client is a veteran or veteran's dependent or a non-VA provider.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☒	VA Employees
☐	Clinical Trainees
☒	VA Contractors
☒	Members of the Public/Individuals
☐	Volunteers

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

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 VHA IVC 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 date to other downstream data consumers,
- Utilizes PowerApps for user data entry to augment other report sources,
- Integrates with EDI gateway to process claims (X12) transactions to include with reports, and
- Processes CCN contractor deliverables to gather information regarding health care delivery.

E. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.

Utilizes PowerApps for user data entry to augment other report sources, integrates with EDI gateway to process claims (X12) transactions to include with reports, and processes CCN contractor deliverables to gather information regarding health care delivery. Ownership data rights stay within VA as there is no external sharing.

F. Are the modules/subsystems only applicable if information is shared?

No.

G. Is the system operated in more than one site to include primary and secondary 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?

Backup data durability is obtained by synchronously replicating data across three databases in different data centers.

3. Legal Authority and System of Record Notices (SORN)

H. What is the citation of the legal authority?

Title 38, United States Code, Sections 501(b) and 304.

Title 38, United States Code, section 7301(a).

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.

I. What is the SORN?

SORN: 24VA10A7, Patient Medical Records - VA (10-2-2020), https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf.

SORN: 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry, and Payment Files - VA (3-3-2015), https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf.

SORN: 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12-23-2020), https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf.

J. SORN revisions/modification

SORNS 24VA10A7 and 79VA10 apply to this system or collection and do not need any updates or modifications.

SORN 54VA10NB3 has been updated from SORN 54VA16. This update relates to the Health Administration Center Civilian Health and Medical Program Records—VA, which is being revised. The revisions encompass updates to the following sections: System Name, System Number, System Location, Categories of Individuals Covered by the System, Categories of Records in the System, Authority for Maintenance of the System, Purpose, and Routine Uses of the Records Maintained in the System. Additionally, the updates address Categories of Users and their associated Purposes: Retrievability, Safeguards, Retention and Disposal, System Manager(s) and Address, Record Access Procedure, and Notification

Procedure. For a comprehensive understanding of these changes, refer to the Federal Register at the designated sites:

- https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf
- Federal Register :: Privacy Act of 1974; System of Records

K. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

The EPRS system is not in the process of being modified.

4. System Changes

L. Will the business processes change due to the information collection and sharing?

☐ *Yes*
☒ *No*

If yes,

M. Will the technology changes impact information collection and sharing?

☐ *Yes*
☒ *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 Information collected, used, disseminated, created, or maintained in the system.

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority to Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

☒ Name
☒ **Full** Social Security Number
☒ **Partial** Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☒ Financial Information
☒ Health Insurance Beneficiary Numbers Account Numbers
☒ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☒ Tax Identification Number
☒ Medical Record Number
☒**Sex**
☒ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Date of Death
☐ Business Email Address
☒ Electronic Data Interchange Personal Identifier (EDIPI) ☒ Other Data Elements (list below)

Other PII/PHI data elements:

- Provider Data {Name, address, National Provider Identifier (NPI)}
- Benefits Information
- Marital Status
- Relationship to Veteran
- Member ID
- Claim Data
- Referrals
- Claims Payments
- City
- State
- Zip Code
- Drug Enforcement Agency (DEA) Number
- Licensed State

1.2 List 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?

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

EPRS sources data from the CDW and external CCN Contractors and stores the retrieved data for further processing and reporting. In addition, through the EPRS PowerApps, users can enter data related to contract variances.

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.

EPRS data sources are VA Cooperate Data Warehouse (CDW), where the VA stores all patient and medical data. The external Community Care Network (CCN) Contractors are the sources that generate the data.

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

EPRS collects detailed data for reports utilizing the VA Corporate Data Warehouse (CDW) data, which holds all patient and medical information. This data is produced by external Community Care Network (CCN) contractors.

1.3 Methods of information collection

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?

EPRS gathers data from the CDW and external CCN Contractors.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

Not Applicable (N/A). EPRS does not collect data on a form therefore is not subject to the Paperwork Reduction Act.

1.4 Information checks for accuracy, and 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.

EPRS is dependent on data consistency checks performed by the CDW and third-party contractors that it relies on for data. 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.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

EPRS does not check for accuracy by accessing a commercial aggregator of information. The quantity of the data received is based on each deliverable expected. The systems responsibility is to maintain and ensure the data is complete and protected.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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

SORN: 24VA10A7, Patient Medical Records - VA (10-2-2020), https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf, Legal Authority: Title 38, United States Code, Sections 501(b) and 304.

SORN: 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3-3-2015), https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf, Legal Authority: 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.

SORN: 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12-23-2020), https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf, Legal Authority: Title 38, United States Code, section 7301(a).

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:

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

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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: VA employees utilize PII information in the EPRS System, including connections to the Corporate Data Warehouse (CDW). Risks include misuse of PII and inaccuracy of data.

Mitigation: Security audit logging, controlled access via Azure JIT, and very limited persistent access for a few select individuals limit the risk of internal abuse of PII data in Azure. The Azure Privacy Officer is responsible for establishing policies and procedures to safeguard privacy across Azure services. All staff in an engineering role are required to take the annual training on standards of business conduct, which includes security and privacy. Contractors operate under NDAs, contractors with access to customer data and PII must sign additional contract addendums that ensure they understand and agree to Azure's privacy and data handling policies. Azure does not share PII data with other federal customers.

Section 2. Uses of the Information

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

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

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

Data Elements Table

PII/PHI Data Element	Internal Use	External Use
Veterans and/or Dependents Data:	**NOTE: EPRS is not the definitive source for the collected information and does not comprehend the specific purposes for which the authoritative source(s) gathered that data.**	
Name	EPRS only collects and stores this data- no other internal use.	Not used
Date of Birth (DOB)	EPRS only collects and stores this data- no other internal use.	Not used
Race and/or Ethnicity	EPRS only collects and stores this data- no other internal use.	Not used
Electronic Data Interchange Personal Identifier (EDIPI)	EPRS only collects and stores this data- no other internal use.	Not used

Sex	EPRS only collects and stores this data- no other internal use.	Not used
Integrated Control Number (ICN)	EPRS only collects and stores this data- no other internal use.	Not used
Date of Death	EPRS only collects and stores this data- no other internal use.	Not used
Partial Social Security Number	EPRS only collects and stores this data- no other internal use.	Not used
Social Security Number	EPRS only collects and stores this data- no other internal use.	Not used
Personal Mailing Address	EPRS only collects and stores this data- no other internal use.	Not used
Personal Phone Number(s)	EPRS only collects and stores this data- no other internal use.	Not used
Personal Email Address	EPRS only collects and stores this data- no other internal use.	Not used
Emergency Contact Information	EPRS only collects and stores this data- no other internal use.	Not used
Financial Account Information	EPRS only collects and stores this data- no other internal use.	Not used
Certificate/License numbers	EPRS only collects and stores this data- no other internal use.	Not used
Health Insurance Beneficiary Numbers	EPRS only collects and stores this data- no other internal use.	Not used
Current Medications	EPRS only collects and stores this data- no other internal use.	Not used
Previous Medical Records	EPRS only collects and stores this data- no other internal use.	Not used
Tax Identification Number (TIN)	EPRS only collects and stores this data- no other internal use.	Not used
Medical Record	EPRS only collects and stores this data- no other internal use.	Not used
Medical Record Number	EPRS only collects and stores this data- no other internal use.	Not used
Member ID	EPRS only collects and stores this data- no other internal use.	Not used
Claims Data	EPRS only collects and stores this data- no other internal use.	Not used
Claims Payments	EPRS only collects and stores this data- no other internal use.	Not used
Referrals	EPRS only collects and stores this data- no other internal use.	Not used
Benefit Information	EPRS only collects and stores this data- no other internal use.	Not used
Marital Status	EPRS only collects and stores this data- no other internal use.	Not used
Relationship to Veteran	EPRS only collects and stores this data- no other internal use.	Not used
Provider Data [Name, address, National Provider Identifier (NPI)]	EPRS only collects and stores this data- no other internal use.	Not used
VA Employees Data:	**NOTE: EPRS is not the definitive source for the collected information and does not comprehend the specific purposes for which the authoritative source(s) gathered that data.**	

Name	EPRS only collects and stores this data- no other internal use.	Not used
Personal Mailing Address	EPRS only collects and stores this data- no other internal use.	Not used
Personal Phone Number	EPRS only collects and stores this data- no other internal use.	Not used
VA Contractors Data:	**NOTE: EPRS is not the definitive source for the collected information and does not comprehend the specific purposes for which the authoritative source(s) gathered that data.**	
Name	EPRS only collects and stores this data- no other internal use.	Not used
Personal Mailing Address	EPRS only collects and stores this data- no other internal use.	Not used
Personal Phone Number	EPRS only collects and stores this data- no other internal use.	Not used
Members of the Public/Individuals Data:	**NOTE: EPRS is not the definitive source for the collected information and does not comprehend the specific purposes for which the authoritative source(s) gathered that data.**	
Name	EPRS only collects and stores this data- no other internal use.	Not used
City	EPRS only collects and stores this data- no other internal use.	Not used
State	EPRS only collects and stores this data- no other internal use.	Not used
Zip Code	EPRS only collects and stores this data- no other internal use.	Not used
National Provider Identifier (NPI)	EPRS only collects and stores this data- no other internal use.	Not used
Tax Identification Number (TIN)	EPRS only collects and stores this data- no other internal use.	Not used
Non-VA Provider Data:		
Name	EPRS only collects and stores this data- no other internal use.	Not used
City	EPRS only collects and stores this data- no other internal use.	Not used
State	EPRS only collects and stores this data- no other internal use.	Not used
Zip Code	EPRS only collects and stores this data- no other internal use.	Not used
National Provider Identifier (NPI)	EPRS only collects and stores this data- no other internal use.	Not used
Drug Enforcement Agency (DEA) Number	EPRS only collects and stores this data- no other internal use.	Not used
License Number	EPRS only collects and stores this data- no other internal use.	Not used
Licensed State	EPRS only collects and stores this data- no other internal use.	Not used

2.2 Describe the types of tools 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?

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 Office of Community Care (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).

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.

EPRS 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. EPRS acts as facilitator of data to other downstream data consumers.

2.3 How the information in the system is 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?

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.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

All EPRS SSN data is stored on encrypted hard drives.

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

FIPS-140-2 encryption using TLS v1.2, and storage of data in an encrypted Azure Virtual Machine Data Disk. Azure SQL Database (PaaS) is encrypted by default from MAG cloud.

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 to the EPRS system is granted solely at the discretion of an EPRS administrator. Access is provided on a need-to-know basis. VA staff members must complete an Access Request Form, which requires signatures from both the requester and the employee's supervisor for approval. The local Office of Information Technology (OIT) verifies that staff members have completed the Privacy and Cyber Security Training and the Signed Rules of Behavior by signing the Access Request Form. This completed form is then sent to a designated email group. Once the OIT has signed the Access Request Form, access is granted by the administrators.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Yes, the VA- 6500 handbook is used as guidance. All EPRS documentation regarding access controls are documented in policy and procedure and/or SOPs documents which are stored within secure SharePoint sites as well as within EMASS.

2.4c Does access require manager approval?

Yes. The Access Request Form must be signed by the employee's supervisor and OIT for approval.

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

Role-based security is implemented in the application to ensure that the data is only accessible to the users through the secure Power Apps interface. Access is restricted to the EPRS system

administrators. PII/PHI/SPI is protected in the application and only presented to users identified as having access to PII/PHI/SPI.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

Employees, supervisor, EPRS administrator(s), and OIT.

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

PII/PHI Data Element:

- Veteran and/or Dependent Name
- Veteran and/or Dependent Date of Birth
- Veteran and/or Dependent Race and/or Ethnicity
- Veteran and/or Dependent Electronic Data Interchange Personal Identifier (EDIPI)
- Veteran and/or Dependent Sex
- Veteran and/or Dependent Integrated Control Number (ICN)
- Veteran and/or Dependent Date of Death
- Veteran and/or Dependent Partial Social Security Number
- Veteran and/or Dependent Social Security Number
- Veteran and/or Dependent Personal Mailing Address
- Veteran and/or Dependent Personal Phone Number(s)
- Veteran and/or Dependent Personal Email Address
- Veteran and/or Dependent Emergency Contact Info
- Veteran and/or Dependent Financial Account Info
- Veteran and/or Dependent Certificate/License numbers
- Veteran and/or Dependent Health Insurance Beneficiary Numbers
- Veteran and/or Dependent Current Medications
- Veteran and/or Dependent Previous Medical Records
- Veteran and/or Dependent Tax Identification Number (TIN)
- Veteran and/or Dependent Medical Record
- Veteran and/or Dependent Medical Record Number
- Veteran and/or Dependent Member ID
- Veteran and/or Dependent Claims Data
- Veteran and/or Dependent Claims Payments
- Veteran and/or Dependent Referrals
- Veteran and/or Dependent Benefit Information
- Veteran and/or Dependent Marital Status

- Veteran and/or Dependent Relationship to Veteran
- Veteran and/or Dependent Provider Data {Name, address, National Provider Identifier (NPI)}
- VA Employee Name
- VA Employee Personal Mailing Address
- VA Employee Personal Phone Number
- VA Contractors Name
- VA Contractors Personal Mailing Address
- VA Contractors Personal Phone Number
- Members of the Public/Individuals Name
- Members of the Public/Individuals City
- Members of the Public/Individuals State
- Members of the Public/Individuals Zip Code
- Members of the Public/Individuals National Provider Identifier (NPI)
- Members of the Public/Individuals Tax Identification Number (TIN)
- Non- VA Provider City
- Non- VA Provider State
- Non- VA Provider Zip Code
- Non- VA Provider National Provider Identifier (NPI)
- Non- VA Provider Name
- Non- VA Provider Drug Enforcement Agency (DEA) Number
- Non- VA Provider License Number
- Non- VA Provider Licensed State

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

VA RCS 1260.1

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.

a. Unscanned Records. All documents maintained in paper form.
    - Disposition Instruction: Temporary. Destroy 6 years after all individuals in the record become ineligible for program benefits.
    - Disposition Authority: N1-15-03-1, item 1.

b. Input Scanned Records. Paper source documents that have been scanned for electronic media storage (optical disk).
   - Disposition Instruction: Temporary. Destroy after successfully scanned to electronic medium.
   - Disposition Authority: N1-15-03-1, item 2.
c. Electronic Records. (Master Files) Electronic records produced from scanned documents or records received electronically (optical disk, magnetic tape or other electronic medium).
   - Disposition Instruction: Temporary. Destroy 6 years after all individuals in the record become ineligible for program benefits.
   - Disposition Authority: N1-15-03-1, item 3.
d. Output document. Paper copies of documents generated from electronic files.
   - Disposition Instruction: Temporary. Destroy when no longer needed.
   - Disposition Authority: N1-15-03-1, item 4.
e. Backup-duplicate files. Electronic copies retained in case the master file is damages or inadvertently erased.
   - Disposition Instruction: Temporary. Delete when identical records have been captured in a subsequent backup/duplicate file.
   - Disposition Authority: N1-15-03-1, item 5.
f. Documentation Records. Data system specifications, codebooks, record layouts, data dictionaries, etc.
   - Disposition Instruction: Temporary. Destroy when superseded or obsolete.
   - Disposition Authority: N1-15-03-1, item 6.
g. Electronic Indexes. Indexes used to provide access to electronic files.
   - Disposition Instruction: Temporary. Delete when related files are no longer needed.
   - Disposition Authority: N1-15-03-1, item 7.

3.3 The retention schedule 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. Please work with the system 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, and here are the disposition numbers: N1-15-03-1, item 1, N1-15-03-1, item 2, N1-15-03-1, item 3, N1-15-03-1, item 4, N1-15-03-1, item 5, N1-15-03-1, item 6, N1-15-03-1, item 7.

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

VHA Records Control Schedule (RCS 10-1) VA RCS 1260.1, Care in the Community.

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.

The EPRS database will be deleted six (6) years after all individuals in the record become ineligible for program benefits. This follows 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. 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 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

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

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

Principle of Minimization: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

Principle of Data Quality and Integrity: The PIA should describe policies and procedures for how PII that is no longer relevant and necessary is purged.
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: There is a risk that the information contained in the EPRS system will be retained for longer than is necessary to fulfill the VA Mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To combat the risk of PII and SPI being breached, the EPRS system will follow RCS 10-1 and VA RCS 1260.1, 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 PII Mapping of Components

4.1a EPRS consists of 6 key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by EPRS and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9a in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
EPRS Database (SQL Server DB (VM) and Azure PaaS database)	Yes	Yes	Veterans and/or Dependents Data: • Name • Date of Birth (DOB) • Race and/or Ethnicity • Electronic Data Interchange Personal Identifier (EDIPI) • Sex • Integrated Control Number (ICN) • Date of Death • Partial Social Security Number • Social Security Number • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact Information • Financial Account Information • Certificate/License numbers	Stored for data aggregation reporting.	Stored in encrypted VA Enterprise Cloud (VAEC) databases. Audit logging. Control access, Azure just-in-time.

			• Health Insurance Beneficiary Numbers • Current Medications • Previous Medical Records • Tax Identification Number (TIN) • Medical Record • Medical Record Number • Member ID • Claims Data • Claims Payments • Referrals • Benefit Information • Marital Status • Relationship to Veteran • Provider Data [Name, address, National Provider Identifier (NPI)] VA Employees Data: • Name • Personal Mailing Address • Personal Phone Number VA Contractors Data: • Name • Personal Mailing Address • Personal Phone Number Members of the Public/Individuals Data: • Name • City • State • Zip Code • National Provider Identifier (NPI) • Tax Identification Number (TIN) Non-VA Provider Data: • Name • City • State • Zip Code • National Provider Identifier (NPI) • Drug Enforcement Agency (DEA) Number • License Number • Licensed State		
1 Pre-Prod Windows 2019 MS SQL Server	Yes	Yes	Veterans and/or Dependents Data: • Name • Date of Birth (DOB) • Race and/or Ethnicity • Electronic Data Interchange Personal Identifier (EDIPI) • Sex	Stored for data aggregation reporting.	Stored in encrypted VA Enterprise Cloud (VAEC) databases. Audit logging. Control access, Azure just-in-time.

			• Integrated Control Number (ICN) • Date of Death • Partial Social Security Number • Social Security Number • 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 (TIN) • Medical Record • Medical Record Number • Member ID • Claims Data • Claims Payments • Referrals • Benefit Information • Marital Status • Relationship to Veteran • Provider Data [Name, address, National Provider Identifier (NPI)] VA Employees Data: • Name • Personal Mailing Address • Personal Phone Number VA Contractors Data: • Name • Personal Mailing Address • Personal Phone Number Members of the Public/Individuals Data: • Name • City • State • Zip Code • National Provider Identifier (NPI) • Tax Identification Number (TIN) Non-VA Provider Data: • Name • City • State • Zip Code		

			• National Provider Identifier (NPI) • Drug Enforcement Agency (DEA) Number • License Number • Licensed State		
Microsoft Power Application Interface	Yes	No	Non-VA Provider Data: • Name • City • State • Zip Code • National Provider Identifier (NPI) • Drug Enforcement Agency (DEA) Number • License Number • Licensed State	Collected for data aggregation reporting.	Dataverse databases are using SQL TDE (Transparent Data Encryption, compliant with FIPS 140-2) to provide real-time I/O encryption and decryption of the data and log files for data encryption at-rest. Azure uses industry standard transport protocols such as TLS between user devices and Microsoft data centers, and within data centers themselves. To protect data even more, internal communication between Microsoft services is using Microsoft backbone network and therefore is not exposed to the public internet.
DAS interface (API)	Yes	No	Veterans and/or Dependents Data: • Name • Date of Birth (DOB) • Race and/or Ethnicity • Electronic Data Interchange Personal Identifier (EDIPI) • Sex • Integrated Control Number (ICN) • Date of Death • Partial Social Security Number • Social Security Number • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact Information • Financial Account Information	Collected for data aggregation reporting.	TLS 2.0, FIPS 140-2

			• Certificate/License numbers • Health Insurance Beneficiary Numbers • Current Medications • Previous Medical Records • Tax Identification Number (TIN) • Medical Record • Medical Record Number • Member ID • Claims Data • Claims Payments • Referrals • Benefit Information • Marital Status • Relationship to Veteran • Provider Data [Name, address, National Provider Identifier (NPI)] VA Employees Data: • Name • Personal Mailing Address • Personal Phone Number VA Contractors Data: • Name • Personal Mailing Address • Personal Phone Number Members of the Public/Individuals Data: • Name • City • State • Zip Code • National Provider Identifier (NPI) • Tax Identification Number (TIN)		
Azure Data Factory (ADF)	Yes	No	Veterans and/or Dependents Data: • Name • Date of Birth (DOB) • Race and/or Ethnicity • Electronic Data Interchange Personal Identifier (EDIPI) • Sex • Integrated Control Number (ICN) • Date of Death • Partial Social Security Number • Social Security Number • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address	Collected for data aggregation reporting.	TLS 2.0, FIPS 140-2

			• Emergency Contact Information • Financial Account Information • Certificate/License numbers • Health Insurance Beneficiary Numbers • Current Medications • Previous Medical Records • Tax Identification Number (TIN) • Medical Record • Medical Record Number • Member ID • Claims Data • Claims Payments • Referrals • Benefit Information • Marital Status • Relationship to Veteran • Provider Data [Name, address, National Provider Identifier (NPI)] VA Employees Data: • Name • Personal Mailing Address • Personal Phone Number VA Contractors Data: • Name • Personal Mailing Address • Personal Phone Number Members of the Public/Individuals Data: • Name • City • State • Zip Code • National Provider Identifier (NPI) • Tax Identification Number (TIN) Non-VA Provider Data: • Name • City • State • Zip Code • National Provider Identifier (NPI) • Drug Enforcement Agency (DEA) Number • License Number • Licensed State		
SQL Server Integration	Yes	No	Veterans and/or Dependents Data: • Name	Collected for data	TLS 2.0, FIPS 140-2

Service (SSIS) Process			• Date of Birth (DOB) • Race and/or Ethnicity • Electronic Data Interchange Personal Identifier (EDIPI) • Sex • Integrated Control Number (ICN) • Date of Death • Partial Social Security Number • Social Security Number • 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 (TIN) • Medical Record • Medical Record Number • Member ID • Claims Data • Claims Payments • Referrals • Benefit Information • Marital Status • Relationship to Veteran • Provider Data [Name, address, National Provider Identifier (NPI)] VA Employees Data: • Name • Personal Mailing Address • Personal Phone Number VA Contractors Data: • Name • Personal Mailing Address • Personal Phone Number Members of the Public/Individuals Data: • Name • City • State • Zip Code • National Provider Identifier (NPI)	aggregation reporting.	

			• Tax Identification Number (TIN) Non-VA Provider Data: • Name • City • State • Zip Code • National Provider Identifier (NPI) • Drug Enforcement Agency (DEA) Number • License Number • Licensed State		

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT system	List PII/PHI data elements shared/received/transmitted.	Describe the method of transmittal
Veterans Health Administration (VHA) / Corporate Data Warehouse (CDW)	Collected for data aggregation reporting.	Veterans and/or Dependents Data: Name, Date of Birth (DOB), Race and/or Ethnicity, Electronic Data Interchange Personal Identifier (EDIPI), Sex, Integrated Control Number (ICN), Date of Death, Partial Social Security Number, Social Security Number, Personal Mailing Address,	Secure VA Network (HTTPS or TLS) Azure Express Route (AER) (encrypted)

IT system and/or Program office. Information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT system	List PII/PHI data elements shared/received/transmitted.	Describe the method of transmittal
		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 (TIN), Medical Record, Medical Record Number, Member ID, Claims Data, Claims Payments, Referrals, Benefit Information, Marital Status, Relationship to Veteran, Provider Data [Name, address, National Provider Identifier (NPI)] VA Employees Data: Name, Personal Mailing Address, Personal Phone Number VA Contractors Data: Name, Personal Mailing Address, Personal Phone Number Members of the Public/Individuals Data: Name, City, State, Zip Code, National Provider Identifier (NPI), Tax Identification Number (TIN) Non-VA Provider Data: Name, City, State, Zip Code, National Provider Identifier (NPI), Drug Enforcement Agency (DEA) Number, License Number, Licensed State	VAEC Trusted Internet Connections (TIC)
Veterans Health Administration (VHA) / Health Share Electronic Data Interchange (EDI)	EDI Gateway used to translate and parse X12 837 files.	Veterans and/or Dependents Data: Name, Date of Birth (DOB), Race and/or Ethnicity, Electronic Data Interchange Personal Identifier (EDIPI), Sex, Integrated Control Number (ICN), Date of Death, Partial Social Security Number, Social Security Number, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information,	Secure VA Network (HTTPS or TLS) Azure Express Route (AER) (encrypted) VAEC Trusted Internet Connections (TIC)

IT system and/or Program office. Information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT system	List PII/PHI data elements shared/received/transmitted.	Describe the method of transmittal
		Financial Account Information, Certificate/License numbers, Health Insurance Beneficiary Numbers, Current Medications, Previous Medical Records, Tax Identification Number (TIN), Medical Record, Medical Record Number, Member ID, Claims Data, Claims Payments, Referrals, Benefit Information, Marital Status, Relationship to Veteran, Provider Data [Name, address, National Provider Identifier (NPI)]	
Veterans Health Administration (VHA) / Active Directory	Single Sign-On (SSO) and for selecting Business Owner & Assigned COR	VA Employees Data: Name, Personal Mailing Address, Personal Phone Number	VA Network
Veterans Health Administration (VHA) / Community Care Reimbursement System (CCRS)	Sharing 835 and 837 files.	Claims, Referrals, Payments	Secure VA Network (HTTPS or TLS) Azure Express Route (AER) (encrypted) VAEC Trusted Internet Connections (TIC)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with	List the purpose of information being shared / received / transmitted	List the specific PII/PHI data elements that are processed (shared/received/transmitted)	List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)	List the method of 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.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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

Follow the format below:

Privacy Risk: There is no external sharing.

Mitigation: There is no external sharing.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

The Community Care Clinical and BI Solution – Enterprise Reporting System Assessing does not collect data directly.

The PIA is public notice to the collection and use of this information.

The following SORNs are public notice to the collection and use of this information:

- SORN: 24VA10A7, Patient Medical Records

- SORN: 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry, and Payment Files
- SORN: 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records.

6.1b If notice was not provided, explain why.

The Community Care Clinical and BI Solution – Enterprise Reporting System Assessing does not collect data directly. The PIA is public notice to the collection and use of this information.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

The Community Care Clinical and BI Solution – Enterprise Reporting System Assessing does not collect data directly. The PIA is public notice to the collection and use of this information.

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.

The Community Care Clinical and BI Solution – Enterprise Reporting System Assessing does not collect data directly, therefore opt-out is determined at the main system of collection.

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.

The Community Care Clinical and BI Solution – Enterprise Reporting System Assessing does not collect data directly. Restriction is used as the source of the data.

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 Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

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

<u>Principle of Transparency:</u> This is referring to sufficient notice provided to the individual.

<u>Principle of Use Limitation:</u> The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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: EPRS does not collect information directly from individuals. 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 procedure 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 Champ VA Guidebook.

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 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

The system does not directly collect PII/PHI however the 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.

7.1b 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)?

EPRS is not the owner of the information, information access request must be made to the owner of the information.

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?

EPRS is not the owner of the information, information access request must be made to the owner of the information.

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.

The system does not directly collect PII/PHI however 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 system does not directly collect PII/PHI however 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. ***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.

The system does not directly collect PII/PHI however 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.*** *(Work with your Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

Privacy Risk: Access to the EPRS System is unavailable therefore could cause a denial to the Veteran/Beneficiary for 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. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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?

Access to the EPRS system is granted solely at the discretion of an EPRS administrator. Access is provided on a need-to-know basis. VA staff members must complete an Access Request Form, which requires signatures from both the requester and the employee's supervisor for approval. The local Office of Information Technology (OIT) verifies that staff members have completed the Privacy and Cyber Security Training and the Signed Rules of Behavior by signing the Access Request Form. This completed form is then sent to a designated email group. Once the OIT has signed the Access Request Form, access is granted by the administrators.

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?

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.

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.

There are a variety of user roles which 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.

8.2a. Will VA contractors have access to the system and the PII?

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.
- Certain contractors maintaining the information system have elevated access to the EPRS database to be able to support various development and maintenance activities.

8.2b. What involvement will contractors have with the design and maintenance of the system?

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.
- Certain contractors maintaining the information system have elevated access to the EPRS database to be able to support various development and maintenance activities.

8.2c. Does the contractor have a signed confidentiality agreement?

No, LITS/Booz Allen sign a Business Associate Agreement, as well as Rules of Behavior (ROB) for annual training that address PHI/PII.

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

Yes, LITS/Booz Allen has a BAA with the VA and is found on the Privacy Services website.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?

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.

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 access 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 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 HIPPA 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 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed and approved.
2. *The System Security Plan Status Date:* 12/4/2024
3. *The Authorization Status:* Authorized for 2-year ATO.
4. *The Authorization Date:* 1/27/2022
5. *The Authorization Termination Date:* 1/25/2027
6. *The Risk Review Completion Date:* 1/13/2025
7. *The FIPS 199 classification of the system:* High.

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

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

This question does not apply to EPRS system because the authorization and accreditation has already been completed as marked above.

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. ***(Refer to question 1.8 of the PTA)***

The EPRS web-based application system is hosted by the VA Enterprise Cloud (VAEC) Azure. EPRS front-end is Microsoft Power Application. EPRS is Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).

9.2 Does the contract with the Hosting 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 3.3.1 of the PTA)***

This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Agreement in place with VA Enterprise Cloud (VAEC) Microsoft Azure Government High (MAG), FedRAMP Package #: F1603087869, Microsoft Azure Government High-FedRAMP approved.

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.
This question is related to privacy control DI-1, Data Quality.

The EPRS system does not collect ancillary data.

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.

This is not applicable to us in this case as the EPRS contract, we are not a cloud provider.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

The EPRS system does not utilize RPA.

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**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

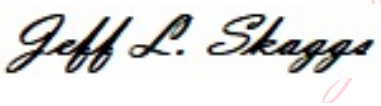
Signature of Responsible Officials

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

ELLER PAMINTUAN

Digitally signed by ELLER PAMINTUAN
Date: 2025.04.18 07:08:45 -06'00'

Privacy Officer, Eller Pamintuan



Digitally signed by JEFFREY SKAGGS
Date: 2025.04.18 06:17:13 -07'00'

Information System Security Officer, Jeffrey Skaggs

TONY SINES

Digitally signed by TONY SINES
Date: 2025.04.18 08:24:28 -05'00'

Information System Owner, Tony Sines

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

The following link, Privacy Act System of Records Notices (SORNs) is where the SORNs listed in Section 6 can be found:

- 24VA10A7, Patient Medical Records.
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry, and Payment Files.
- 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records.

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04:
Notice of Privacy Practices
VHA Notice of Privacy Practices is located here:
VHA Notice of Privacy Practices

EPRS Privacy Impact Analysis link: EPRS PIA Folders.

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)