Privacy Impact Assessment for the VA IT System called:

Provider Profile Management System (PPMS)

Veterans Health Administration (VHA)

Office of Integrated Veteran Care (IVC)

Date PIA submitted for review:

07/14/2023

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)	Kimberly Keene	kimberly.keene@va.gov	401-248-5933
Information System Owner	Dena Liston	Dena.liston@va.gov	304-886-7367

Abstract

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

Provider Profile Management System (PPMS) is a comprehensive repository of administrative information and is the authoritative source of Non-VA Providers for VHA. The PPMS Customer Relationship Management tool provides a layer of validation of the non-VA provider data and supports workflow management and tracking. PPMS is comprised of the Integrated Web Service, Data Web Service, and the Provider Integration Engine. The system also hosts the PPMS Provider Locator used to identify available Community Care providers in a mapped proximity to a Veterans location for scheduling care.

Overview

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

1 General Description

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

Provider Profile Management System (PPMS) is owned by the VHA Office of Integrated Veteran Care (IVC).

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

Provider Profile Management System (PPMS) focuses on the implementation of the non-VA care provider directory employed by multiple VA portfolios such as: Community Care Network (CCN), TriWest Patient-Centered Community Care (PC3) and Choice Program, Veteran Care Agreements (VCA), VA Medical Center Local Contracts, Indian Health Service (IHS) Providers, Department of Defense (DOD) facilities and VA Medical Center providers. As the authoritative source of non-VA provider data, downstream systems rely on PPMS to complete their own business process to support the Veteran. PPMS is a comprehensive repository of administrative information and the authoritative source of Non-VA Providers for VHA offering validation and collection of other non-VA provider information as well as allowing for workflow management and tracking.

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

VA Controlled / non-VA Owned and Operated
VHA Office of Integrated Veteran Care (IVC)

2. Information Collection and Sharing

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

There are currently 1.3 million non-VA provider's information stored in PPMS. Non-VA providers would be medical providers in the Community that do not directly work for Veteran's Affairs.

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

The Provider Profile Management System (PPMS) is a comprehensive repository of information of VA community providers. PPMS will collect and retain personally identifiable information on non-VA health care providers, specifically the provider's Tax Identification Number (TIN), which can sometimes be their Social Security Number, in order to facilitate payment(s) to the provider when they render service to a qualified veteran or beneficiary. VA Provider publicly available data is retained in the system, no personally identifiable information is collected on VA providers. These providers will be conducting health services with the Department of Veterans Affairs which maintains a directory of medical providers internal to the Veterans Affairs Medical Centers (VAMC) and external Community Care (CC) providers to be used by the multiple portfolios in maintaining the Community Care Provider Network. The non-VA care providers date of birth, tax identification number and/or Social Security Number will be collected by the CCN contractors and submitted electronically directly to PPMS via PPMS secure Integrated Web Services (IWS). A second method of collecting the date is by the Support Assistants (MSA), Program Support Assistants (PSA), Registered Nurses (RN), and social workers (Geriatrics and Extended Care (GEC)) at the local VA facility. PPMS will provide increased timeliness and quality service to Veterans by improved tracking of provider relationships and validating data elements, as well as enterprise wide accessibility to a comprehensive list of provider information for referrals and scheduling Community Care services for Veterans.

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

The data in the system is shared with other systems with the use of Data Web Services (DWS) as well as personnel through the PPMS Repository Customer Relationship (CRM) tool.

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.

PPMS is a cloud-based application. The repository is accessed by logging into the system using the Microsoft D365 Active Directory authentication protocol for secured access via Personal identity Verification (PIV) card. PPMS is a repository hosted on the Microsoft Azure Government (MAG) Cloud for provider records which are received electronically from the Community Care Networks (CCN). The CCN's collect the provider data, including the date of birth and tax identification number/social security number, directly from the provider and stores it in a mechanism outside of the VA. The records are electronically transmitted from the CCN to the VA using secure integrated web services where they are stored in PPMS behind the VA firewall.

3. Legal Authority and SORN

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Public Law 104–191; 5 U.S.C. 301; 38U.S. Code § 1703; 45 Code of Federal Regulations (CFR) part 164; and 4 CFR 103.
186VA10D, Community Care (CC) Provider Profile Management System (PPMS) - VA 1/25/2021

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

The PPMS System is not in the process of being modified.

D. System Changes

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

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

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

The completion of this PIA will not result in technology changes.

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

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

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

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

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

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

PII Mapping of Components (Servers/Database)

Provider Profile Management System (PPMS) consists of 1 key components (servers/databases). This component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by PPMS and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VA Corporate Data Warehouse CC_PIE Provider Integration Engine (PIE)	Yes	Yes	Social Security number (SSN), and Date of	As a comprehensive repository of information of VA community providers, PPMS will	Electronically pushed and pulled from A Network FIPS 2.0 Encryption

			Birth (DOB)	**collect and retain personally identifiable information on non-VA health care providers, which would include a tax identification number and or Social Security number for payment processing purposes.**	

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Provider Integration Engine (PIE) features a web-based, automated integration engine. The required data to support PIE resides in VA Corporate Data Warehouse (CDW) database. VA provider data is pulled from CDW.

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.

The Tax Identification numbers (TIN)/Social Security Numbers for non-VA providers to process and ensure payment(s) to the provider when they render services. The Date of Birth is collected/used for verification and identification of the non-VA provider.

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

The PPMS system does not create information.

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

PIE extracts VA provider data from the various CDW tables and aggregates them into the PIE database.

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

Information is not collected on a form and is not subject to the Paperwork Reduction Act.

1.4 How will the information be checked for accuracy? How often will it be checked?

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.

PPMS does not own or manage the information; it inducts it from CDW. Any verification/update/maintenance of the information is the responsibility of CDW.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

The PPMS system does not check for accuracy by accessing a commercial aggregator of information.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

VA Privacy Service has determined the Privacy Act of 1974, 5 U.S.C. § 552a (e), Section 208©, E-Government Act of 2002 (P.L. 107-347), and the Office of Management and Budget (OMB) Circular A-130, Appendix I are the legal authority to permit the collection, use, maintenance and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need. Authority to Operate (ATO) granted on December 3, 2020, for 3 years through December 3, 2023. System Name: Provider Profile Management System (PPMS) Assessing, System Identification Number: 931.
186VA10D, Community Care (CC) Provider Profile Management System (PPMS) - VA 1/25/2021.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: If the Provider Profile Management System (PPMS) receives data that does not comply with required information, fails validation, or was not sent using the expected format from Community Care Third Party Administrators for Regions 1-5, their information will not be ingested into the PPMS system.

Mitigation: The Community Care Third Party Administrators for Regions 1-5 will be notified. Community Care Third Party Administrators for Regions 1-5 will then send corrected updates/changes to the PPMS system via a file update.

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.

PPMS utilizes provider's information to ensure proper processing of payment to the provider when they render service to a qualified veteran or beneficiary.

SSN: May be used as a Tax Identification Number of Provider.
TIN: Required by PPMS for non-VA Providers to be entered into the PPMS System.
DOB: May be used as an identifier for non-VA Providers.

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

The PPMS system does not perform any kind of analysis or run analytic tasks in the background.

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.

The PPMS system does not perform any kind of analysis or run analytic tasks in the background.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

VA protects moderate and high impact information at rest / in transit unless encrypting the data is technically infeasible; or would negatively affect VA ability to carry out missions, functions, or operations.

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

Access to the PII is only approved by Supervisor/Super User, who provides validation for VA employees for provisioned access to PPMS.

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

The VA is responsible for assuring the safeguards for PII are in place for PPMS. This is performed by conducting annual security reviews and ensuring that the system maintains a valid Authorization to Operation (ATO).

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 PII is only approved by Supervisor/Super User, who provides validation for VA employees for provisioned access to PPMS.

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

Access controls for PPMS for protecting the confidentiality, integrity, and availability of the system and the information processed, stored, and transmitted by system. These controls are documented within the PPM System Security Plan.

2.4c Does access require manager approval?

All access to PPMS requires manager approval.

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

The PPMS maintains audit logs that monitor and log access to the system.

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

The VA is responsible for assuring the safeguards for PII are in place for PPMS. This is performed by conducting annual security reviews and ensuring that the system maintains a valid Authorization to Connect (ATO).

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*

Tax Identification Number/SSN and Date of Birth

3.2 How long is information retained?

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

Section 1150-Office of Quality and Performance, electronic records: Temporary. Delete 30 years after the last episode of employment, appointment, contract, etc. from VA. Section 1150.1 Health Care Provider Credentialing and Privileging Records; 1150.2 Health Care Providers not selected for VA employment; electronic records Temporary. Delete 2 years after non-selection or when no longer needed for reference, whichever is sooner.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA Records Officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.
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?

VHA Records Control Schedule 10-1: https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf
Section 1150-Office of Quality and Performance, electronic records: Temporary. Delete 30 years after the last episode of employment, appointment, contract, etc. from VA.

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

POLICIES AND PRACTICES FOR RETENTION AND

DISPOSAL OF RECORDS:

Record Control Schedule (RCS) 10–1 item 1150 Office of Quality and Performance 1150.1. Health Care. Provider Credentialing and Privileging Records. Electronic Files. Electronic version of information entered directly into the electronic credentialing and privileging record information system. Temporary; delete 30 years after the last episode of employment, appointment, contract, etc. from VA. (N1–015–10–07, Item 1) https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01510.pdf

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.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Office of Information and Technology (OIT) MP-6 Electronic Media Sanitization Standard Operating Procedure (SOP). Digital media is shredded or sent out for destruction per VA Handbook 6500.1. Link: file:///C:/Users/VHAISA~1/AppData/Local/Temp/1/MicrosoftEdgeDownloads/43443f0b-1e7a-4bd6-8caa-9de7066b933d/Handbook_6500_24_Feb_2021.pdf

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

PPMS does not utilize live or production data for testing.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: As long as and while PPMS is active, there is no risk. If PPMS is no longer an active product, and records are no longer accessible, then there is a risk to recall purposes.

Mitigation: There will need to be a verification that records are maintained in an alternate record-keeping system; otherwise, the records will no longer be accessible.

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)	To provide up-to-date Provider information	Social Security Number (SSN), Date of Birth (DoB)	Electronically pushed and pulled from VA Network

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*
			FIPS 2.0 Encryption
Data Access Service (DAS)	To provide up-to-date Provider information	Social Security Number (SSN), Date of Birth (DoB)	Electronically pulled from VA Network FIPS 2.0 Encryption
VA Employees	To provide up-to-date Provider information	Social Security Number (SSN), Date of Birth (DoB)	Manually entered into VA Network FIPS 2.0 Encryption
Community Care Reimbursement System (CCRS)	To provide up-to-date Provider information	Social Security Number (SSN), Date of Birth (DoB)	Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption
Community Care Referral and Authorization System (CCRA/HSRM)	To provide up-to-date Provider information	Social Security Number (SSN), Date of Birth (DoB))	Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption
VA.gov	To provide up-to-date Provider information	Social Security Number (SSN), Date of Birth (DoB)	Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption
VistA	To provide up-to-date Provider information	Social Security Number (SSN), Date of Birth (DoB)	Electronically pushed from VA Network FIPS 2.0 Encryption
Community Viewer (CV)	To provide up-to-date Provider information	Social Security Number (SSN), Date of Birth (DoB)	Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption

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*
Cerner	To provide up-to-date Provider information	Social Security Number (SSN), Date of Birth (DoB)	Manual extraction from PPMS within VA Network FIPS 2.0 Encryption
VA Online Scheduling (VAOS)	To provide up-to-date Provider information	Social Security Number (SSN), Date of Birth (DoB)	Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption
Authorization and Eligibility Tool (AET)	To provide up-to-date Provider information	Social Security Number (SSN), Date of Birth (DoB)	Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption
Community Care Provider Locator (CPL)	To provide up-to-date Provider information	Social Security Number (SSN), Date of Birth (DoB)	Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption
Financial Service Center (FSC)	To provide up-to-date Provider information	Social Security Number Social Security Number (SSN), Date of Birth (DoB)	Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: The privacy risk associated with maintaining SPI is that this data may be disclosed to individuals who do not require access, which would increase the risk of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by the PPMS personnel. Only personnel with a clear business purpose are allowed access to the system and to the information contained within.

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	***List the purpose of information being shared /***	***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,***	***List the method of transmission and the measures in***

shared/received with	***received / transmitted with the specified program office or IT system***		***SORN routine use, etc. that permit external sharing (can be more than one)***	***place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: PPMS does not share data directly with external organizations.

Mitigation: PPMS does not share data directly with external organizations.

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Community Care Network (CCN) contractor is collecting data and providing to the VA; therefore, the notice is given by the contractor. Link: https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01510.pdf. 186VA10D, Community Care (CC) Provider Profile Management System (PPMS) – VA (1/25/2021)

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

VA Medical Centers provide data based on the Veteran Care Agreement (VCA), which is solely distributed, collected, and submitted by Third Party Administrators.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

VA Medical Centers provide data based on the Veteran Care Agreement, agreed to by the VA Medical Centers and non-VA Providers.

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.

Providers will go back to the point of collection. Providers have the opportunity and right to decline to provide information.

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.

Providers will go back to the point of collection, which is the Third Party Administrator with such requests.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: Non-VA Providers do not receive notification of Privacy Practices at the point of collection, which is the responsibility of the Third-Party Administrators collecting data (Provider Data Vendors).

Mitigation: Non-VA Provider's information will not be accepted or ingested into PPMS without written proof of receipt of notification of Privacy Practices.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Information collected in PPMS can be accessed under the FOIA and Privacy Act. VA FOIA Regulation for this is documented in the VA Handbook 6300.3 Procedures for Implementing the Freedom of Information Act. FOIA requests may be submitted to VHA.IVC.FOIA@va.gov and Privacy Act requests for personal documents may be submitted to VHA.IVC.PO@va.gov. Link to FOIA: https://vapal.efoia-host.com/.

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).

PPMS is not exempt from the access provisions of the Privacy Act.

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.

PPMS is a Privacy Act system.

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 information would be corrected at the point of collection, which would then come downstream to PPMS. System of Record Notification (SORN) Community Care (CC) Provider Profile Management System (PPMS) pending 186VA10D – See link below:
https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01510.pdf

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 information would be corrected at the point of collection, which would then come downstream to PPMS. System of Record Notification (SORN) Community Care (CC) Provider Profile Management System (PPMS) 186VA10D – See link below:
https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01510.pdf

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 information would be corrected at the point of collection, which would then come downstream to PPMS. System of Record Notification (SORN) Community Care (CC) Provider Profile Management System (PPMS) 186VA10D – See link below:
https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01510.pdf

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that erroneous information may be provided to PPMS from the point of collection.

Mitigation: Inform or refer to the point of collection. PPMS does not collect data directly from the providers.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

Access to PPMS is granted based on role-based access control.

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?

There are no identified users from other agencies that have access to PPMS.

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.

Accounts Payable personnel: PPMS users with access to view the TIN (SSN) data for non-VA providers to ensure proper processing of payments. System Administrators: Privileged users tasked with maintaining the PPMS system and making authorized functional changes to it and/or data. Database Administrators: Privileged users tasked with maintaining the PPMS database system and making authorized data changes to the database. They also perform the integration and loading of data between PPMS and data repositories.

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.

No, VA contractors do not have access to the system and the PII. VA employees have access to the system and the PII.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

All PPMS users undergo annual VA Privacy training. Completion of this training annually is required to obtain a VA account which is needed to access PPMS. The following training is applicable to all or role-specific users: Privacy and Security Training (all users) VA 10176: Privacy and Info Security Awareness and Rules of Behavior; VA 10203: Privacy and HIPAA Training. 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

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

YES

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 10/08/2020
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 12/03/2020
5. *The Authorization Termination Date:* 12/03/2023
6. *The Risk Review Completion Date:* 09/15/2021
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* MODERATE

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

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

N/A

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

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

Microsoft Azure Government Cloud (MAG)

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

VA118-16-D-1001 36C10B18N1001006 P00031

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

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

This question is related to privacy control DI-1, Data Quality.

No, the CSP will not collect any 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.

A Statement of Work (SOW) or Performance Work Statement (PWS) will be written to establish privacy roles and responsibilities for contractors if they are required to have access to PHI/PII.

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 PPMS system is not utilizing Robotics Process Automation.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

MICHAEL HARTMANN

Digitally signed by MICHAEL HARTMANN
Date: 2023.08.01 12:36:43 -06'00'

Privacy Officer, Michael Hartmann

KIMBERLY KEENE

Digitally signed by KIMBERLY KEENE
Date: 2023.08.07 15:16:15 -04'00'

Information Systems Security Officer, Kimberly Keene

DENA LISTON

Digitally signed by DENA LISTON
Date: 2023.08.07 15:57:00 -04'00'

Information Systems Owner, Dena Liston

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

186VA10D, Community Care (CC) Provider Profile Management System (PPMS) – VA (1/25/2021)

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices