Privacy Impact Assessment for the VA IT System called:

Provider Profile Management System (PPMS)

VHA Office of Community Care (OCC)

**Date PIA submitted for review:**

February 23, 2021

**System Contacts:**

<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Julie Drake</td>
<td><a href="mailto:julie.drake@va.gov">julie.drake@va.gov</a></td>
<td>(303) 331-7823</td>
</tr>
<tr>
<td>Information System</td>
<td>Kimberly Keene</td>
<td><a href="mailto:kimberly.keene@va.gov">kimberly.keene@va.gov</a></td>
<td>(401) 248-5933</td>
</tr>
<tr>
<td>Security Officer (ISSO)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information System</td>
<td>Christopher Brown</td>
<td><a href="mailto:christopher.brown1@va.gov">christopher.brown1@va.gov</a></td>
<td>(202) 270-1432</td>
</tr>
</tbody>
</table>
Abstract

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

The PPMS will provide a standardized method for VA to collect and establish Master Provider Consolidation Repository to gain information from multiple provider entities, which currently does not exist, and a standardized method for managing and analyzing provider data to support accurate, data driven decision making for improving provider relations and provider network management.

Overview

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

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes
- Whether the completion of this PIA could potentially result in technology changes
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?
- Does the system use cloud technology? 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.
- Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?
- 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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?
The Community Care (CC) 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.

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 collects 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.

PPMS is estimated to have about 2M+ providers by Q3 of 2021. The typical Provider record includes: First Name, Middle Initial, Last Name, Provider Identifier - National Provider Index number (NPI), Tax ID, Status (Active/Non-Active), Quality Score, Ranking Score, email address, Address (work location), phone number (work), fax number, Affiliations (facilities), and additional provider related information.

PPMS is not a regional GSS, VistA, or LAN.
PPMS is a Major Application in eMASS.
System Name: Provider Profile Management System (PPMS) Assessing
System Identification: 931

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.

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.

Legal authority to operate the IT system.
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

System of Record Notification (SORN) Community Care (CC) Provider Profile Management System (PPMS) 186VA10D – [Federal Register, Volume 86 Issue 14 (Monday, January 25, 2021)](govinfo.gov)

The approval of this PIA will not require changes to existing business processes. It will complement the current activities conducted in the field outside of the PPMS system. Completion of the PIA would not result in required technology changes. This system is not in the process of being modified and at this time a SORN does not exist. System of Record Notification (SORN) Community Care (CC) Provider Profile Management System (PPMS) 186VA10D – See link here: [Federal Register, Volume 86 Issue 14 (Monday, January 25, 2021)](govinfo.gov)

The system is designed, developed, and deployed in production on the Microsoft Azure Government (MAG) cloud. FedRamp status of the application is inherited from the MAG cloud with D365 service which received approval on 4/29/20.

VA Enterprise Cloud (VAEC) provides the enterprise level hosting environment and Dynamics 365 platform for PPMS. The VAEC has a Master Services Agreement. It is established that VA retain ownership rights over the data hosted in the cloud including the PII portions of the record.

VA Enterprise Cloud (VAEC) provides the enterprise level hosting environment and Dynamics 365 platform for PPMS. The VAEC has a Microsoft Enterprise Agreement (EA) Performance Work Statement (PWS) which has language for the cloud provider to ensure security and privacy of the data held.

The PII data considered in this scenario is only if a Provider uses their Social Security Number as the TAXID for payment purposes. Disclosure of this information would be moderate harm causing reputational damage to the VA as this type of data breach has occurred in the past for other VA systems.

**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/](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.

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
- [x] Social Security Number
- [x] Date of Birth
- [ ] Mother’s Maiden Name
- [ ] Personal Mailing Address
- [ ] Personal Phone Number(s)
- [ ] Personal Fax Number
- [ ] Personal Email Address
- [ ] Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- [ ] Financial Account Information
- [ ] Health Insurance Beneficiary Numbers
- [ ] Account numbers
- [ ] Certificate/License numbers
- [ ] Vehicle License Plate Number
- [ ] Internet Protocol (IP) Address Numbers
- [ ] Current Medications
- [ ] Previous Medical Records
- [ ] Race/Ethnicity
- [ ] Tax Identification Number
- [ ] Medical Record Number
- [x] Other Unique Identifying Number (list below)

No Veteran/Beneficiary PII/PHI is collected in this system. Provider Social Security Number and provider Date of Birth

**PII Mapping of Components**

PPMS consists of 1 key component. 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.

**PII Mapped to Components**

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA Corporate Data Warehouse vhacdwdwhsql52 database name CC_PIE Provider Integration Engine (PIE)</td>
<td>Yes</td>
<td>Yes</td>
<td>Provider social security number (SSN), and Date of Birth (DOB)</td>
<td>As a comprehensive repository of information of VA community providers, PPMS will collect and safeguard</td>
<td>PPMS is a customized Microsoft Dynamics 365 solution deployed on a FedRAMP Accredited Microsoft platform</td>
</tr>
</tbody>
</table>
1.2 What are the sources of the information in the system?

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

Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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.

1.3 How is the information collected?

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

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.
PIE extracts VA provider data from the various CDW tables and aggregates them into the PIE database.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose. This question is related to privacy control AP-2, Purpose Specification.

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.

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

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract. This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

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.

1.6 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

System of Record Notification (SORN) Community Care (CC) Provider Profile Management System (PPMS) pending 186VA10D – See link here: 2021-01510.pdf (govinfo.gov)

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information
Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

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 sent using the expected format from Community Care Third Party Administrators for Regions 1-5,

Mitigation:
THEN the Vendor will be notified via a transaction response file of the error. Vendor is then responsible to send updates/changes to the PPMS system.
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.

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

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

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

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

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

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

Consider the following FIPPs below to assist in providing a response:
**Principle of Transparency:** Is the PIA and SORN, if applicable, clear about the uses of the information?

**Principle of Use Limitation:** Is the use of information contained in the system relevant to the mission of the project?

*This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.*

Add answer here:

**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.

**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.

**Does access require manager approval?** All access to PPMS requires manager approval.

**Is access to the PII being monitored, tracked, or recorded?** The PPMS maintains audit logs that monitor and log access to the system.

**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*

All information checked in question 1.1 is retained:

- Date of Birth
- Tax Identification Number/SSN

**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. 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)? If so please indicate the name of the records retention schedule.

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

VHA Records Control Schedule 10-1: [https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf](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.

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.

3.4 What are the procedures for the elimination of SPI?

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

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

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.

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. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

*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**

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
</table>
| 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 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 |
<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Care Reimbursement System (CCRS)</td>
<td>To provide up-to-date Provider information</td>
<td>Social Security Number (SSN) • Date of Birth (DoB)</td>
<td>Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption</td>
</tr>
<tr>
<td>Community Care Referral and Authorization System (CCRA/HSRM)</td>
<td>To provide up-to-date Provider information</td>
<td>Social Security Number (SSN) • Date of Birth (DoB)</td>
<td>Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption</td>
</tr>
<tr>
<td>VA.gov</td>
<td>To provide up-to-date Provider information</td>
<td>Social Security Number (SSN) • Date of Birth (DoB)</td>
<td>Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption</td>
</tr>
<tr>
<td>VistA</td>
<td>To provide up-to-date Provider information</td>
<td>Social Security Number (SSN) • Date of Birth (DoB)</td>
<td>Electronically pushed from VA Network FIPS 2.0 Encryption</td>
</tr>
<tr>
<td>Community Viewer (CV)</td>
<td>To provide up-to-date Provider information</td>
<td>Social Security Number (SSN) • Date of Birth (DoB)</td>
<td>Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption</td>
</tr>
<tr>
<td>Decision Support Tool (DST)</td>
<td>To provide up-to-date Provider information</td>
<td>Social Security Number (SSN) • Date of Birth (DoB)</td>
<td>Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption</td>
</tr>
<tr>
<td>Consult Tool Box (CTB)</td>
<td>To provide up-to-date Provider information</td>
<td>Social Security Number (SSN) • Date of Birth (DoB)</td>
<td>Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption</td>
</tr>
<tr>
<td>Cerner</td>
<td>To provide up-to-date Provider information</td>
<td>Social Security Number (SSN) • Date of Birth (DoB)</td>
<td>Manual extraction from PPMS within VA Network FIPS 2.0 Encryption</td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared/received with the specified program office or IT system</td>
<td>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>VA Online Scheduling (VAOS)</td>
<td>To provide up-to-date Provider information</td>
<td>Social Security Number (SSN)  • Date of Birth (DoB)</td>
<td>Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption</td>
</tr>
<tr>
<td>Authorization and Eligibility Tool (AET)</td>
<td>To provide up-to-date Provider information</td>
<td>Social Security Number (SSN)  • Date of Birth (DoB)</td>
<td>Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption</td>
</tr>
<tr>
<td>Community Care Provider Locator (CPL)</td>
<td>To provide up-to-date Provider information</td>
<td>Social Security Number (SSN)  • Date of Birth (DoB)</td>
<td>Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption</td>
</tr>
<tr>
<td>Financial Service Center (FSC)</td>
<td>To provide up-to-date Provider information</td>
<td>Social Security Number (SSN)  • Date of Birth (DoB)</td>
<td>Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption</td>
</tr>
<tr>
<td>Authorization and Eligibility Tool (AET)</td>
<td>To provide up-to-date Provider information</td>
<td>Social Security Number (SSN)  • Date of Birth (DoB)</td>
<td>Electronically pulled from PPMS Data Web Service (DWS) within VA Network FIPS 2.0 Encryption</td>
</tr>
</tbody>
</table>

### 4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Follow the format below:

**Privacy Risk:**
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: This question is #7 in the Privacy Threshold Analysis.

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

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.
1. PPMS is categorized in accordance with FIPS 199 and NIST SP 800-60 to ensure proper categorization to identify any PII and level of security controls needed to protect it.

2. The VA has security policies which direct and guide data protection activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.

3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.

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:
N/A, PPMS does not share data directly with external organizations.

Mitigation:
N/A, 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 notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.
If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

Community Care Network (CCN) contractor is collecting data and providing to the VA; therefore, the notice is given by the contractor.

VA Medical Centers provide data based on the Veteran Care Agreement (VCA).

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.

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.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:
Privacy Risk:
If 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:
Then it is the responsibility of the Vendor to provide notification of Privacy Practices to the Provider.

Section 7. Access, Redress, and Correction

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

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

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

If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

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.OCC.FOIA@va.gov and Privacy Act requests for personal documents may be submitted to VHA.OCC.PO@va.gov.

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.
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.

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

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

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

The information would be corrected at the point of collection, which would then come downstream to PPMS.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

**Principle of Individual Participation:** Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

**Principle of Individual Participation:** Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

*This question is related to privacy control IP-3, Redress.*

Follow the format below:

**Privacy Risk:**
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?**

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

Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

*Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.*

*This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.*

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

End Users: PPMS users that are analyzing provider data to support accurate, data driven decision making for improving provider relations and provider network management.

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 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

Version Date: February 27, 2020
Page 22 of 26
8.4 Has Authorization and Accreditation (A&A) been completed for the system?

If Yes, provide:

1. **The date the Authority to Operate (ATO) was granted**
   12/03/2020
2. **Whether it was a full ATO or ATO with Conditions,**
   FULL ATO
3. **The amount of time the ATO was granted for**
   12/03/2023 (3 years)
4. **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.

If No or In Process, provide your **Initial Operating Capability (IOC) date.**
### Section 9. References

**Summary of Privacy Controls by Family**

#### Summary of Privacy Controls by Family

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

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

JULIE C. DRAKE
969177
Digitally signed by JULIE C. DRAKE 969177
Date: 2021.04.15 08:48:06 -06'00'

Privacy Officer, Julie Drake

Kimberly D. Keene 106407
Digitally signed by Kimberly D. Keene 106407
Date: 2021.04.15 10:41:23 -04'00'

Information Systems Security Officer, Kimberly Keene

Christopher Brown 101386
Digitally signed by Christopher Brown 101386
Date: 2021.04.15 08:27:08 -05'00'

System Owner, Christopher Brown
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).

SORN link: https://www.oprm.va.gov/docs/Current_SORN_List_02_02_2021.pdf