Privacy Impact Assessment for the VA IT System called:

# Patient Context Management

## Veterans Health Administration

## Office of Health Informatics

## eMASS ID # 2332

Date PIA submitted for review:

04/02/2025

System Contacts:

*System Contacts*

|  | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Nancy Katz-Johnson | Nancy.katz-johnson@va.gov | 203-535-7280 |
| Information System Security Officer (ISSO) | LaWanda Wells | Lawanda.Wells@va.gov | 202-607-8724 |
| Information System Owner | Mark S. Kelley | Mark.Kelley2@va.gov | 737-212-3284 |

# Abstract

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

Patient Context Management (PCM) enables context sharing between applications, by synchronizing and coordinating applications so that they automatically follow the user's context. PCM provides a basis for ensuring secure and consistent access to patient information from heterogeneous sources allowing users to synchronize their views with respect to patient data or other clinical data. This application temporarily utilizes PII to maintain patient context with participating clinical applications.

The PCM servers do not persist any patient information in its storage. The information is resident only in the RAM to the lifetime of the service that's running, so the moment the vault shuts down, there isn't any information on patients.

# Overview

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

*1   General Description*

> A.  *What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*
>
>     PCM enables patient context sharing between applications, by synchronizing and coordinating applications so that they automatically follow the user's context.
>
> B.  *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*
>
>     VA Owned and VA Operated

*2. Information Collection and Sharing*

> C.  *Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*
>
>     The PCM servers do not persist any patient information in its storage. The information is resident only in the RAM to the lifetime of the service that's running so the moment the vault shuts down, there isn't any information on patients.

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

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

The following information, as initiated and collected by one of the 12 interfacing applications, is used by PCM to increase patient safety by synchronizing Veteran's data across all open clinical applications:
- Social Security Number (SSN)
- Date of Birth (DOB)
- Sex
- Name
- Data File Number (DFN)
- Integration Control Number (ICN)
- Alias
- Electronic Data Interchange Personal Identifier (EDIPI)
- Internal Entry Number (IEN)

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

PCM interfaces with the following patient care applications where data is shared:
- Computerized Patient Record System
- Clinical Decision Support Platform
- Scheduling Software (VSE)
- Joint Longitudinal Viewer (JLV)
- VistA Imaging
- Bar Code Medication Administration
- VistA Nursing Vitals Measurements
- After Visit Summary
- Taylor Communications iMedConsent Web
- Medtronics Omnivisor Pro
- Home Telehealth – Cognosante

- CP Flow Sheets

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

Yes, the modules/subsystems are applicable because the system receive, store, or share data with the component/modules/subsystems.

G. *Is the system operated in more than one site to include primary and secondary site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?*

The system is hosted in AWS GovCloud (US).

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

H. *What is the citation of the legal authority?*

The information in PCM is not retrieved by a personal identifier and therefore does not require a SORN under the Privacy Act. The source data is Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (79VA10). AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, section 7301(a).

I. *What is the SORN?*

This system does not require a SORN.

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

N/A

*4. System Changes*

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

☐ Yes
☒ No
*if yes, <<ADD ANSWER HERE>>*

I. *Will the technology changes impact information collection and sharing?*

☐ Yes
☒ No
*if yes, <<ADD ANSWER HERE>>*

# Section 1. Characterization of the Information

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

**1.1 Information collected, used, disseminated, created, or maintained in the system.**

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

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

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

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

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

---

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

Other PII/PHI data elements: Data File Number (DFN), Alias, Internal Entry Number (IEN)

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

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

The PII is transmitted by the interfacing application user as entered in their application.

*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.*

No sources other than those of the interfacing applications are required.

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

The system does not create information.

## 1.3 Methods of information collection
*These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

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

Data elements used for context management are encrypted in transit and not identifiable.

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

Information is not collected on a form.

## 1.4 Information checks for accuracy, and how often will it be checked.
*These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.*

*1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.*

Data is not stored in the system however regarding the source data, most of the information provided by veterans or other members of the public, such as address and phone number, next of kin and emergency contact information, and similar information are assumed to be accurate because it is provided directly by the individual. Additionally, information entered an individual's medical record by a doctor or other medical staff is also assumed to be accurate and is not verified

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

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

**1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.**

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

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under 45 CFR § 164.502 (3) and 45 CFR § 164.510.

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

*Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.*

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

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

*<u>Principle of Minimization:</u> The information is directly relevant and necessary to accomplish the specific purposes of the program.*

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

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

Follow the format below when entering your risk assessment:

**Privacy Risk:** PCM processes Personally Identifiable Information (PII). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, personal, professional, or financial harm may result for the individuals affected.

**Mitigation:** The VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Our overall security controls follow VA 6500 Handbook, and NIST SP800-53 high impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of the VA's hosting facility's common security controls. The operating system is scanned monthly, the system undergoes annual security audits including but not limited to Fortify, WASA, and network penetration testing if applicable.

# Section 2. Uses of the Information

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

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

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

| PII/PHI Data Element | Internal Use | External Use |
|---|---|---|
| Social Security Number (SSN) | File Identification purposes | Not used |
| Date of Birth (DOB) | Context Management purposes | Not used |
| Sex | Context Management purposes | Not used |
| Name | Context Management purposes | Not used |
| Data File Number (DFN) | Context Management purposes | Not used |
| Integration Control Number (ICN) | Context Management purposes | Not used |
| Alias | Context Management purposes | Not used |
| Electronic Data Interchange Personal Identifier (EDIPI) | Context Management purposes | Not used |
| Internal Entry Number (IEN) | Context Management purposes | Not used |

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

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

The system uses specific identifier data entered in the interfacing application to create a match with other context-enabled applications. No other data is analyzed or created from this process.

*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 PCM system does not create, store, or make available new or unutilized information into systems participating in clinical context.

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

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

Data elements used for context management are encrypted in transit. The PCM servers do not persist any patient information in its storage.

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

No other protections are in place to protect SSNs beyond the encryption while in transit.

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

Data elements used for context management are encrypted in transit.

## 2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

*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?*

PCM does not have access to PII information. This access is controlled through the application participating in clinical context.

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

All criteria, procedures, controls and responsibilities regarding access are documented through the application participating in clinical context.

*2.4c Does access require manager approval?*

No, all access is controlled by the application participating in clinical context.

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

Access to the PII is monitored, tracked or recorded by the application participating in clinical context.

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

The information is handled in accordance with the uses described above include mandatory online information security and Privacy and HIPAA training; face-to-face training for all incoming new employees conducted by the Information System Security Officer and Privacy Officer; regular audits of individuals accessing sensitive information; and formal administrative rounds during which personal examine all areas within the facility to ensure information is being appropriately used and controlled.

All VA employees are required to complete annual Rule of Behavior training; however, since the data that passes through the system is secured with government-approved encryption, it's not possible for that data to be viewed by personnel.

# 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*

The PCM servers do not retain any patient information in storage.

## 3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule [https://www.archives.gov/records-mgmt/grs](https://www.archives.gov/records-mgmt/grs)? This question is related to privacy control DM-2, Data Retention and Disposal.*

No information is retained by the system; however, information resides in the RAM. Application context is retained in memory as long as the participant (clinical application) is reachable by vault. This is determined by a handshake every 30 seconds, which is configurable. In a situation that the vault does not receive a ping message from client for an application participant and after retry attempts (effectively 60 seconds), the vault removes the clinical application context from its memory (RAM).

## 3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

*An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. Please work with the system VA Records Officer to answer these questions.*
*This question is related to privacy control DM-2, Data Retention and Disposal.*

*3.3a Are all records stored within the system of record indicated on an approved disposition authority?*

Yes, all records are stored within the system of records as per this disposition authority: GENERAL RECORDS SCHEDULE 5.2: Transitory and Intermediary Records

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

GENERAL RECORDS SCHEDULE 5.2: Transitory and Intermediary Records
[https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf](https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf)

Item 020, Disposition instructions: Temporary. Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later.
DAA-GRS-2022-0009-0002

## 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.*

No information is retained by the system, thus nothing to eliminate or transfer.

## 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.*

No PII data is used in testing or training. Fictitious data (test patients) is used to accomplish this.

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

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

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

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

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

Follow the format below:

**Privacy Risk:**
System misconfiguration could lead to PII being at risk.

**Mitigation:**
This is a cloud-based system where the Cloud Service Provider Third Party Assessment Organization (CSP 3PAO) already conducts penetration testing and defense in depth. Flaw remediation is centrally managed through four separate processes: -- The deployment of antivirus configurations to all system servers -- The use of configuration management to centrally manage the identification of all required Red Hat Enterprise Linux (RHEL) patches and to install them on appropriate servers. Monthly Nessus scanning informs system staff of required security vulnerabilities and fixes. Scanning results are reported, analyzed, and recorded for remediation. Systems are backed up continuously to an alternate site. Monthly Security Configuration Compliance Data (SCCD) scans are conducted using the BigFix tool to validate secure configuration of the software.

# Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

**PII Mapping of Components**

4.1a **Patient Context Management** consists of **1** key component (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Patient Context Management** and the reasons for the collection of the PII are in the table below.

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

*Internal Components Table*

| Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI | Does this system collect PII? (Yes/No) | Does this system store PII? (Yes/No) | Type of PII (SSN, DOB, etc.) | Reason for Collection/ Storage of PII | Safeguards |
|---|---|---|---|---|---|
| Context Manager | Yes | No | SSN, Name, DOB, Sex, ICN, DFN | Support VA mission requirements | Encryption at Rest and in Transit |

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

**NOTE: Question 3.9b (second table) on Privacy Threshold Analysis should be used to answer this question.**

*Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.*

*State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.*

*For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.*

*Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?*
*This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.*

*Data Shared with Internal Organizations*

| *IT system and/or Program office. Information is shared/received with* | *List the purpose of the information being shared /received with the specified program office or IT system* | *List PII/PHI data elements shared/received/transmitted.* | *Describe the method of transmittal* |
|---|---|---|---|
| Computerized Patient Record System | Support VA mission requirements | Name, DOB, Sex, ICN, DFN | SSL |
| Clinical Decision Support Platform | Support VA mission requirements | Name, DFN, ICN | SSL |
| Scheduling Software (VSE) | Support VA mission requirements | DFN, ICN | SSL |
| Joint Longitudinal Viewer (JLV) | Support VA mission requirements | Name, EDIPI, ICN, IEN | SSL |
| VistA Imaging | Support VA mission requirements | SSN (full), Name, DOB, Sex, ICN, DFN | SSL |
| Bar Code Medication Administration | Support VA mission requirements | SSN (partial), Name, DOB, Sex, ICN, DFN | SSL |
| VistA Nursing Vitals Measurements | Support VA mission requirements | ICN, DFN | SSL |
| After Visit Summary | Support VA mission requirements | DFN, Name | SSL |
| Taylor Communications iMedConsent Web | Support VA mission requirements | DFN | SSL |

| IT system and/or Program office. Information is shared/received with | List the purpose of the information being shared /received with the specified program office or IT system | List PII/PHI data elements shared/received/transmitted. | Describe the method of transmittal |
|---|---|---|---|
| Medtronics Omnivisor Pro | Support VA mission requirements | DFN | SSL |
| Home Telehealth - Cognosante | Support VA mission requirements | ICN, DFN | SSL |
| CP Flow Sheets | Support VA mission requirements | Name, DOB, DFN, ICN | SSL |

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

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

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

Follow the format below:

**Privacy Risk:**
The internal sharing of data is necessary for individuals to receive VHA benefits, however, there is a risk that the data could be shared with an inappropriate VA organization or institution which could result in a breach of privacy and disclosure of PII/PHI to unintended parties or recipients.

**Mitigation:**
Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.

## Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

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

**The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, please**

**describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.**

**NOTE:  Question 3.10 on Privacy Threshold Analysis should be used to answer this question.**

*Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.*

*For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.*

*What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?*

*Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.*
*This question is related to privacy control UL-2, Information Sharing with Third Parties*

*Data Shared with External Organizations*

| *List IT System or External Program Office information is shared/received with* | *List the purpose of information being shared / received / transmitted* | *List the specific PII/PHI data elements that are processed (shared/received/transmitted)* | *List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)* | *List the method of transmission and the measures in place to secure data* |
|---|---|---|---|---|
| N/A | N/A | N/A | N/A | N/A |

## 5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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

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

*Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.*

*Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.*
*This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing*

Follow the format below:

**Privacy Risk:** There is no external sharing.

**Mitigation:** There is no external sharing.

## Section 6. Notice

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

**6.1 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.**
*These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.*

*6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.*

The VHA Notice of Privacy Practice (NOPP) explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non-Veterans receiving care are provided the notice at the time of their encounter.

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

This Privacy Impact Assessment (PIA) also serves as notice as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

*6.1b If notice was not provided, explain why.*

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

VPCM does not collect data directly from the individual, but rather by the VA employee utilizing one of the 12 interfacing systems.  The Notice of Privacy Practice given to the individual explains the uses of their information.

**6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?**

*This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.*

Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

Employees and VA contractors are also required to provide the requested information to maintain employment or their contract with *VHA.*

**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.*

Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

Information is used in accordance with the Privacy Act and is shared with VA employees when the information is needed in accordance with job requirements or when there is authority under b(1) of the Privacy Act. In addition, individuals may consent to additional uses of the information. >>

**6.4 PRIVACY IMPACT ASSESSMENT: Notice**

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

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

*Principle of Transparency: This is referring to sufficient notice provided to the individual.*

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

Follow the format below:

**Privacy Risk:**  There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.

**Mitigation:**   This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records, The NOPP is also available at all VHA medical centers from the facility Privacy Officer.

Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

## Section 7. Access, Redress, and Correction

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

**7.1 The procedures that allow individuals to gain access to their information.**
*These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.*

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

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

There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office.

VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access.VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records. Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact Contract Officer Representative (COR) to obtain information upon request.

*7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?*

Information is not retrieved by a personal identifier and therefore it is not under the Privacy Act however the source documents are covered by 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?*

 Individuals can obtain access to the source documents in accordance with the Privacy Act.

## 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.*

Patient Context Manager does not retain information however individuals can request correction of the source documents in accordance with the Privacy Act.

## 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.*

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) which states:

**Right to Request Amendment of Health Information.**
You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.

Additional notice is provided through the SORS which serves as the source document for the information and this PIA.

**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.*

Redress is provided as indicated above.

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

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

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

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

Follow the format below:

**Privacy Risk:**  There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

**Mitigation:**   The risk of incorrect information in an individual's records is mitigated by authenticating information, when possible, Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.
The NOPP discusses the process for requesting an amendment to one's records.

The Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information.

The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

## Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

**8.1 The procedures in place to determine which users may access the system, must be documented.**
*These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.*

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

System administrators must submit an Elevated Privileges request and be approved by an authorizing official before access to the system can be granted.

*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?*

User from other agencies do not have access to the system.

*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.*

Only system administrators have access to the system.

**8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.**

*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.*

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

> There are no contractors working on the system so no confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed

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

> VA contractors will not have access to the system and the PII.

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

> Contractors will not be involved with the design and maintenance of the system

**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 VA personnel are required to complete annual VA Privacy and Information Security Awareness and Rules of Behavior training; however, although the system handles PII, it's not accessible by users of the system. Basic HIPPA training is covered under the Privacy and Information Security training.

**8.4 The Authorization and Accreditation (A&A) completed for the system.**

*8.4a If completed, provide:*

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 02/02/2024
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 11/22/2024
5. *The Authorization Termination Date:* 11/22/2025
6. *The Risk Review Completion Date:* 10/28/2024
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 not completed or In Process, provide your **Initial Operating Capability (IOC) date.***

    NA


## Section 9 – Technology Usage

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

**9.1 Does the system use cloud technology? If so, what cloud model is being utilized?**
*If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.* **(Refer to question 1.8 of the PTA)**

    The system is an Infrastructure as a Service utilized within the VA Enterprise Cloud (VAEC) boundary.

**9.2  Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract).** **(Refer to question 3.3.1 of the PTA)** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

    The system is hosted in VAEC AWS GovCloud. Contract #NNG15SD22B

**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.*

    VA has full ownership of any ancillary data stored in the system as it's hosted in VAEC AWS GovCloud.

**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.*

VAEC ensures security and privacy of any data held.

**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 system does not utilize 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 |

| ID | Privacy Controls |
|---|---|
| DM-3 | Minimization of PII Used in Testing, Training, and Research |
| **IP** | **Individual Participation and Redress** |
| IP-1 | Consent |
| IP-2 | Individual Access |
| IP-3 | Redress |
| IP-4 | Complaint Management |
| **SE** | **Security** |
| SE-1 | Inventory of Personally Identifiable Information |
| SE-2 | Privacy Incident Response |
| **TR** | **Transparency** |
| TR-1 | Privacy Notice |
| TR-2 | System of Records Notices and Privacy Act Statements |
| TR-3 | Dissemination of Privacy Program Information |
| **UL** | **Use Limitation** |
| UL-1 | Internal Use |
| UL-2 | Information Sharing with Third Parties |

**Signature of Responsible Officials**

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

_____

**Privacy Officer, Nancy Katz-Johnson**

_____

**Information Systems Security Officer, LaWanda Wells**

_____

**Information Systems Owner, Mark S. Kelley**

## APPENDIX A-6.1

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

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

## HELPFUL LINKS:

[Records Control Schedule 10-1 (va.gov)](#)

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

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

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

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

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