Privacy Impact Assessment for the VA IT System called:

Patient-Centered Management Module (PCMM)

Clinical Services

Veterans Health Administration (VHA)

eMASS ID #1256

Date PIA submitted for review:

<< 11/1/2023 >>

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	LaWanda Wells	lawanda.wells@va.gov	202-632-7905
Information System Owner	Christopher Brown	Christopher.Brown1@va.gov	202-270-1432

Abstract

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

The Patient Centered Management Module (PCMM) Web application assists VA facilities in implementing and monitoring patient and staff assignments. In a Primary Care (PC) setting and, in the Patient-Aligned Care Team (PACT) model, patients are assigned a Primary Care Provider (PCP) who is responsible for delivering essential health care, coordinating all health care services, and serving as the point of access for VA care.

Overview

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

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

Patient-Centered Management Module (PCMM), Veterans Health Administration, Clinical Services

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

Patient Centered Management Module (PCMM) software is currently hosted in the Austin Information Technology Center (AITC.) PCMM, under the Program Office of Enterprise Program Management Office (EPMO) is a centralized web application that assists VA facilities in implementing and monitoring patient and staff assignments in both primary care and non-primary care teams. The software allows the user to set up and define a team, assign positions to the team, assign staff to the positions, and assign patients to the team. In a Primary Care setting, patients are assigned a care team that consists of a Primary Care Provider (PCP) or Associate Provider (AP), Care Manager, Clinical Associate and Administrative Associate who is responsible for delivering essential health care, coordinating all health care services, and serving as the point of access for specialty care. An estimated 12 million Veterans in VA Medical Center nationwide are registered in PCMM. The system does not use or store PHI. The patient provided information and PACT information is shared with several applications (My HealthEVet (MHV), Joint legacy viewer (JLV), CDW-Corporate Data Warehouse and VSSC – VHA Support Service Center).The PCMM system's legal authority for operating the system, specifically the authority to collect the information listed is the President's Executive Order: Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs, including the Federal Advisory Committee Act, as amended (5 U.S.C. App.). The legal authority for use of the SSN is Title 38, United States Code, Section 501 (SORN 24VA10A7 Patient Medical Record- VA https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

and 79VA10 Veterans Information System Technology and Architecture (VistA) https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf.

C. *Who is the owner or control of the IT system or project?*
VA owned and operated.

2. Information Collection and Sharing

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

All Veterans who request care from VA facilities will have a record within PCMM to track care team makeup for supporting Veteran health needs. Presently there approximately 13,397,213, this number is dynamic as it will continue to grow as more Veterans become enrolled in the VA healthcare system.

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

The information collection are those that distinguish Veterans from one another, allowing for administration of care.

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

PACT (Patient aligned Care Team) data is shared with other VA IT systems via Remote Procedure Calls, web calls, direct DB connections, and data extracts (Cerner-specific). Sharing allows for easy referencing of patient support team makeup.

G. *Is 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?*

The system is operated at an enterprise level across the VA providing care support to Veterans. PII is maintained in the application's database and is upheld consistently through enterprise level access control measures that controls access based upon assigned user roles and access permissions.

3. Legal Authority and SORN

H. *What is the citation of the legal authority to operate the IT system?*

For System of Record Notice (SORN) 24VA10A7 Patient Medical Record-VA, Title 38, United States Code, Sections 501(b) and 304). https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf.

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

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

The system is not in the process of being modified.

4. System Changes

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

No

K. *Will the completion of this PIA could potentially result in technology changes?*

No

Section 1. Characterization of the Information

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

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

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

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

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

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

☐ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☒ Gender
☒ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin

☒ Other Data Elements (list below)
☒ Gender ID
☒ Death Date
☒ Former Last Name
☒ Beeper number
☒ Enrollment Status
☒ Last Visit Date
☒ ICN
☒ IEN
☒ PID
☒ Patient Long ID
☒ Active Duty Status
☒ Primary Eligibility
☒ Primary Eligibility Date

☒ Active Directory Name
☒ Prefix/Suffix
☒ Title
☒ Work Address
☒ Work Email Address
☒ Work Phone Number
☒ Work Beeper Number
☒ Termination Date

PII Mapping of Components (Servers/Database)

PCMM consists of 2 key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by PCMM 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 3.9 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
PCMM_PROD	**No**	**Yes**	first name, middle name, last name, former or maiden name, prefix, suffix, gender, SSN, ICN, IEN, PID, patient long ID, date of birth, date of death, address, email address, beeper or pager number, phone number, enrollment status, active duty, last visit date, primary eligibility, primary eligibility date	**Patient Management**	**VA 6500 Controls in place data is encrypted**

MIRTHDB_PCMM_PROD	**No**	**Yes**	first name, middle name, last name, gender, SSN, ICN, date of birth, date of death, address	**Patient Management**	**VA 6500 Controls in place data is encrypted**

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

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

- VistA
- MPI
- Cerner

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.

For VistA, MPI, Cerner – information from other sources is required due to PCMM need to validate Veteran EHR information in order to generate PACT make-up and maintain current information.

The following applications (My HealthEVet (MHV), Joint legacy viewer (JLV), CDW-Corporate Data Warehouse and VSSC – VHA Support Service Center) consume PCMM PACT data.

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

Yes, PCMM create PACT, Mental, Special and non-VA team data and is the source of truth for patient care in that regard.

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

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

The data source for PCMM is being collected from the existing VistA files and patient requests in person or online at the VAMCs. The information is stored locally and viewable nationally and is based on location.

Data Quality

a) VHA takes reasonable steps to confirm the accuracy and relevance of the PII it collects. VHA tries to collect PII directly from the individual whenever possible, which allows for better confirmation of the accuracy, relevant, timeliness and completeness of the information. If information is collected in person verbally or on a VA form this confirmation happens as part of the process. When information is collected online or through the mail, confirmation of PII is handled through other processes, such as computer matches.

b) All PII is reviewed for accuracy as it is collected and utilized to care for Veterans. Any PII identified or determined to be inaccurate or outdated, or erroneously placed in the wrong record by VHA staff is updated administratively immediately as appropriate. VHA will also update any PII in a Privacy Act system of records pursuant to a granted amendment request from the individual. VHA Directive 1605.01 outlines policy for processing amendment requests. Other policies, such as VHA Handbook 1907.01 outlines how health records are updated including administratively due to errors.

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?

The data in PCMM is being collected from the existing VistA files and patient requests in person or online at the VAMCs. Medical Center staff can also enter the patient information into PCMM.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

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

PCMM provides on demand validation of teams/assignments which enforces established business rules/logic. When an application user is viewing a team and clicks the validation tool button, PCMM will evaluate the team against pre-defined business rules and will report any inconsistencies or potential issues. Additionally, PCMM Web will validate the person class of the staff members assigned to the staff roles associated with the team roles of Primary Care Provider, Associate Provider, Care Manager, and Clinical Associate prior to assignment.

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?

PCMM also provides some rudimentary checks of data as it is entered into the system as described below:

a. Code level input validation (e.g. data format, selection lists) on the user interface and at the database level.

b. Data validation checks within the database for direct user input as well as electronically received data.
c. Role based functionality (ensuring the right person is providing the right information).
d. Code level validation for electronic interfaces (e.g. data format validation).

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

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

Legal authorities for operating the system are:
For System of Record Notice (SORN) 24VA10A7 Patient Medical Record-VA, Title 38, United States Code, Sections 501(b) and 304). https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf.

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

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: PCMM collects 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
Prefix/Suffix	Used as identifier	No External Use
First Name	Used as a patient identifier	No External Use
Middle Name	Used as a patient identifier	No External Use
Last Name	Used as a patient identifier	No External Use
SSN	Used as a patient identifier	No External Use
DoB	Used to identify patient age and confirm patient identity	No External Use
Personal Mailing Address	Used to contact individual	No External Use
email address	Used to contact individual	No External Use
Personal Phone Number	Used to contact individual	No External Use
Gender ID	Used to contact individual	No External Use
ICN	Used as a patient identifier	Used for external integration for the query of data
Death Date	Used to unassign a patient from his team	No External Use
Former Last Name	Used as a patient identifier	No External Use
Beeper Number	Used to contact individual	No External Use
Enrollment Status	Used as identifier	No External Use
Last Visit Date	Used as identifier	No External Use
Primary Eligibility	Used as identifier	No External Use

Primary Eligibility Date	Used as identifier	No External Use
Active Directory Name	Used as identifier	No External Use
Title	Used as personal identifier	No External Use
Work Address	Used to contact individual	No External Use
Work Email Address	Used to contact individual	No External Use
Work Phone Number	Used to contact individual	No External Use
Work Beeper Number	Used to contact individual	No External Use

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

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

PCMM does not analyze or produce patient data. However, PCMM allows for specific data entry of PACT team let FTE and their allocated exam room space. When data are entered in a standardized manner, the information is used to analyze Primary Care capacity, staffing, space, and workload nationally, by Veteran Integrated Service Network (VISN), by VA medical center, and community-based outpatient clinic (CBOC).

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.

We create patient assignments that are placed into a Veteran's EHR (VistA or Cerner). The derived information allows for viewing assigned staff supporting Veterans and informing patient care support decision.

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

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

Database servers are on a Netapp storage array which is data at rest encrypted (FIPS 140-2 compliant) It's encrypted in transit, SSL is used for both the application and web services.

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

PCMM displays only the last 4 digits of the SSN with the notation that the information is sensitive. The database housing the SSNs are also encrypted and any transfer of data including the SSN is done through a secure encrypted method (https).

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

Our facilities employ all security controls in the respective medium impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how veterans' information is used, stored, and protected.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

Lightweight Directory Access Protocol (LDAP) is required in order to pass the PIV Login page before anyone can access PCMM. Users tasked to perform duties within PCMM must request access to the application from the local PCMM Principal Facility Coordinator, the VISN PCMM Point of Contact, or National PCMM Coordinator. When a user is provisioned access, they are assigned a Role and division(s) within the application. Upon sign-in to the PCMM application and searching a patient, the application confirms that the staff member has a VistA instance at the location the patient is "known at." If the user attempts to pull up a patient "known at" a division they do not have assigned to them in VistA, they will be prompted to enter valid VistA access/verify codes. If they do not have access to that VistA instance, they will not be able to bring up patients' profiles. Our facilities employ all security controls in the respective medium impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how veterans' information is used, stored, and protected.

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

Yes.

2.4c Does access require manager approval?

Yes, ePAS and LEAF.

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

Yes, traceability is managed via auditing logs for tracking PII patient information.

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

All required parties that have elevated permissions, identified special roles, and who has access to PII information within PCMM.

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 data in PCMM is being collected from the existing VistA files and patient requests in person or online at the VAMCs. The PCMM system retains no PII but leverages existing databases containing PII.

3.2 How long is information retained?

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

All electronic records are kept indefinitely per Office Inspector General (OIG) guidance.

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

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

proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and 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?

Paper records are not processed within the PCMM functionality. Information stored on electronic storage media are maintained and disposed of in accordance with Records Control Schedule 10–1 https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf, item 6000.2c, as authorized by the National Archives and Records Administration of the United States.

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

PII data is retained in accordance with Records Control Schedule 10–1 https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf, item 6000.2c, disposition authority N1-15-02-3, item 4.

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.

Paper records are not processed within the PCMM functionality. Digital records, which contain SPI, are not purged. The risk of unintentional access of records is mitigated by the enforcement of the security controls on the PCMM systems to limit the access to the data. 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. If a security event has occurred, the response team can take the appropriate actions.

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 VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

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.

Office of Information and Technology (OIT) documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. This documentation and monitoring is performed through the use of Talent Management System (TMS). Access to the any system for research, testing or training is granted to VA clinical staffs and contractors by the local authority within each administrative area staff office.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: All electronic records are kept indefinitely per Office Inspector General (OIG) guidance. The records are kept indefinitely therefore there is a risk of them being unintentionally released.

Mitigation: To mitigate the risk of corruption or deletion posed by information retention, the data is housed in a secure database repository and is shadowed across Linux cluster members and is backed up by the Information Technology Center operations staff. The risk of unintentional release is mitigated by the enforcement of the security controls on the PCMM systems to limit the access to the data.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Health Administration VistA	Push data to VistA so that patient care information generated by PCMM (team assignment make-up) can be shared with other VA IT systems that leverages EHR.	first name, middle name, last name, former last name/maiden name, prefix/suffix, gender, SSN, ICN, IEN, PID, Patient long ID, date of birth, date of death, address, email address, phone number, beeper/pager number, enrollment status, active duty, last visit date, primary eligibility, primary eligibility date	Remote Procedure Call
Veterans Health Administration MyHealtheVet	They pull PCMM PACT and other team information for display in their application	Name, phone, city, state, SSN, BirthDate	HTTPS Web Service Call
Veterans Health Administration	They pull PCMM PACT and other team	Name, phone, city, state, SSN, birthdate	HTTPS Web Service Call

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Joint Legacy Viewer	information for display in their application		

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The 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 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Cerner	Push data to Cerner so that patient care information generated by PCMM (team assignment make-up) can be shared with other VA IT systems that leverage EHR.	first name, middle name, last name, former last name/maiden name, prefix/suffix, gender, SSN, ICN, IEN, PID, Patient long ID, date of birth, date of death, address, email address, phone number, beeper/pager number, enrollment status, active duty, last visit date, primary eligibility, primary eligibility date	MOU	Secure FTP/ Database Connection

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: There is no external sharing.

Mitigation: There is no external sharing

Section 6. Notice

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

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

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

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

The information used by PCMM is collected from other VA records and the following notices apply to them:

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946 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.

System of Record Notices (SORNs):
24VA10A7 Patient Medical Record - VA https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf and 79VA10 Veterans Information System Technology and Architecture (VistA) https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf.

A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority and the conditions under which the information can be disclosed.

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. If it was provided, attach a copy of the current notice.

Notice is provided.

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

The information used by PCMM is collected from other VA records and the following notices apply to them:

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946 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.

System of Record Notices (SORNs):
24VA10A7 Patient Medical Record - VA https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf and 79VA10 Veterans Information System Technology and Architecture (VistA) https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf.

A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority and the conditions under which the information can be disclosed.

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."

6.2 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.

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 the facility Privacy Officer for review and processing.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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

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

<u>Principle of Transparency:</u> 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: 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. The System of Record Notices (SORNs) and 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 What are the procedures that allow individuals to gain access to their information?
These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

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

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 http://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.

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)?

The system is not exempt from individual right of access. The information used by this system originates in other VA records and requestors should be referred to their local VHA facility to obtain copies of records.

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?

PCMM is not a Privacy Act system. The system contains a check to prevent users of the application from accessing their own medical records.

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.

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal
- File a "Statement of Disagreement"
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Individuals seeking information regarding access to and contesting of VA benefits records may write, call or visit the nearest VA regional office.

Additional notice is provided through the SORS listed in 6.1 of this PIA and through the Release of Information Office where care is received.

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.

Formal redress via the amendment process is available to all individuals, as stated in questions 7.1-7.3In addition to the formal procedures discussed in question 7.2 to request changes to one's health record.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that 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.

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

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

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

Access to Patient Centered Management Module (PCMM) will be granted by National and Veterans Integrated Service Network (VISN) PCMM Coordinators and Principal Facility Coordinators (PFC) through the PCMM "User Administration" option using the LEAF process.

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?

Users from other agencies do not have access to PCMM.

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.

PCMM Roles and access permitted are outlined in the tables below.

Role	Description	PCMM Web Assigned Permissions
PCMM Coordinator	Able to utilize all functionality to create, manage and assign to any PCMM team.	PCMM COORDINATOR
PCMM MH Coordinator	Able to utilize all functionality to create, manage and assign to MHTC PCMM teams only.	PCMM MH Coordinator
PCMM Multi-PCP Clinical Approver	Clinicians currently and potentially caring for the patient or their clinical designee responsible for determining whether there is compelling clinical need for Multi-PACT assignments.	PCMM COORDINATOR
PCMM Specialty Coordinator	Responsible for Non-PACT PCMM management, setup and patient assignments.	PCMM Specialty Coordinator
PACT Administrator – Limited View	Able to view all areas within the application except for patient level data	
PACT Administrator – View All	Able to view all areas within the application including patient level data.	
PCMM Clerk	The role assigned for staff members who performs data entry tasks.	PCMM MH Clerk
PCMM MH Clerk	The role assigned for staff members who performs data entry tasks for MH teams only.	
PCMM Reports Only	User access to PCMM reports only	PCMM Administrative Associate
PCMM Specialty Clerk	The role assigned for staff members who performs data entry tasks for Non PACT areas only.	
PCMM Traveling Veteran Coordinator	Facilitates PCMM Multi-PACT requests while acting as the liaison between sending/receiving facilities for traveling veterans needing care coordination and communicates with the TVC at the other facility to obtain/send information.	
PCMM VISN Coordinator	This designated staff member serves as the VISN's PCMM technical expert with the ability to utilize and troubleshoot all areas of the application and has the ability to access and delegate PCMM user permissions and necessary user training.	
PCMM VISN Traveling Veteran Coordinator	Serves as the VISN TVC SME with the ability to act on the VISN's facilities PCMM Multi-PACT requests as needed.	
PCMM Backup Principal Facility Coordinator	Serves as the back up to the Principal Facility Coordinator	
PCMM Principal Facility Coordinator	There is one PCMM Principal Facility Coordinator for each station (parent station and divisions). This designated staff member serves as the facility's PCMM technical expert with the ability to utilize and troubleshoot all areas of the application and has the ability to access and delegate PCMM user permissions and necessary user training.	

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Yes, further details can be found within each contractors SLA with the VA and the appropriate COR.

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.

Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SOR) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA

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

A&A has been completed for PCMM.

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed.
2. *The System Security Plan Status Date:* 9 May 2023
3. *The Authorization Status:* Completed.
4. *The Authorization Date:* 10 October 2023
5. *The Authorization Termination Date:* 9 October 2025
6. *The Risk Review Completion Date:* 4 October 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

Section 9 – Technology Usage

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

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

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

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

No.

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

No.

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

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

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

No.

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.

No.

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).

No.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

PHILLIP CAUTHERS

Digitally signed by PHILLIP CAUTHERS
Date: 2024.01.10 12:19:36 -08'00'

Privacy Officer, Phillip Cauthers

LAWANDA WELLS

Digitally signed by LAWANDA WELLS
Date: 2024.01.17 07:29:53 -05'00'

Information System Security Officer, LaWanda Wells

CHRISTOPHER BROWN

Digitally signed by CHRISTOPHER BROWN
Date: 2024.01.16 12:30:43 -06'00'

Information 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; screen shot of a website collection privacy notice).

VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

SORN 24VA10A7 Patient Medical Record - VA https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

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

HELPFUL LINKS:

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 Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices