



Privacy Impact Assessment for the VA IT System called:

Patient Care Systems Integration Platform (PCSIP)

Veterans Health Administration

Albany Stratton VA Medical Center

eMASS ID #1258

Date PIA submitted for review:

May 15, 2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Anthony Budhram	Anthony.Budhram@va.gov	518-466-7764
Information System Security Officer (ISSO)	Ryan Gordon	ryan.gordon@va.gov	585-364-9890
Information System Owner	Richard Loubriel	Richard.Loubriel@va.gov	518-626-6729

Abstract

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

Patient Care Systems Integration Program (PCSIP) provides multiple facility departments (Surgery, Emergency, Radiology, Laboratory, etc.) integrated workflow to coordinate care and provide scheduling, patient management, and display patient progress tracking from a provider perspective as well as a patient/family perspective. It’s context-based patient information and analytics capabilities improves Strategic Analytics for Improvement and Learning (SAIL) metrics.

PCSIP also hosts a patient engagement mobile application (app), accessed by patients with their personal devices, to enable pre-visit/pre-surgery prep instruction receipt, record compliance and post visit/surgery follow up instruction receipt, record compliance and outcomes (pain/side effects/etc.) as necessary.

PCSIP facilitates bi-directional communication to the Computerized Patient Record System (CPRS) via the Veterans Health Information Systems and Technology Architecture (VistA).

Internal to the VA, staff access the web app via a pc or the mobile app using iPad or iPhone. Externally, patients can access the mobile app utilizing either an Android device or an iPhone/iPad. When the patient is scheduled, they will receive an email and text message to download the mobile app. Once downloaded, they will receive a text message for first log on instructions where they are prompted to change their password at that time. No PHI or PII is ever transmitted to the patient's device. Only pre-op and post-op instructions are transmitted, and the patient can submit outcomes of the surgery or care received back to providers. VA employees, using a VA issued PC, use the web app using their PIV card credentials. Employees using iPad and iPhones sign into the mobile app with derived PIV credentials.

Both the web app and the mobile app can utilize the PIV exemption as approved when necessary.

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?*

PCSIP is an Office of Information Technology (OIT) owned system that is used by Emergency, Surgery, Surgical Specialties, Radiology, Wards and Labs. PCSIP is designed for three (3) purposes: Improve SAIL metrics, Improve Access to Care for Veterans, and Improve patient outcomes.

- 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.*

This is a VA Owned and VA Operated system.

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 number of Veterans or Dependents (patients) will vary based on the capacity and schedule of the facility department (Surgery, Radiology, Emergency, Laboratory, etc.) and the number of patients that facility services.

The number of VA Employees/Clinical Trainees/Contractors (providers) will also vary based on the capacity and schedule of the staffing of each facility department (doctors/nurses in the emergency department, technicians in radiology and labs, etc.).

The number of Members of the Public (caregivers/spouses/etc.) will vary based on whether or not the patient being processed has someone accompanying them.

The information is only in PCSIP for 24 hours before being transferred to the authoritative EHR source of the data.

Check if Applicable	Demographic of Individuals
<input checked="" type="checkbox"/>	Veterans or Dependents
<input checked="" type="checkbox"/>	VA Employees
<input checked="" type="checkbox"/>	Clinical Trainees
<input checked="" type="checkbox"/>	VA Contractors
<input checked="" type="checkbox"/>	Members of the Public/Individuals
<input type="checkbox"/>	Volunteers

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

PCSIP collects identity and medical record information necessary to process and track any given patient through the workflow/treatment steps of any specific department in a facility. This includes provider (doctor/nurse/technician/etc) information, patient and their health information, and any caregiver/spouse information that is accompanying the patient.

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

Patient identifying information is pulled from the authoritative source (VistA). As the patient goes through the visit in that department and completes the steps required, PCSIP is used to record it all and pushes it back to the authoritative EHR for permanent inclusion into the patients' medical record.

CoreyHealth is a mobile application that providers can utilize on VA furnished mobile devices to enter patient information as they complete the steps in the department visit. The mobile application feeds directly into the mobile application server that communicates with the other system components to compile the information that is pushed back to the EHR.

Varian ARIA is a system used by Radiation Oncology to treat cancer patients. Since ARIA resides in a separate environment in the VA, PCSIP is intended to provide authentication mechanisms as a middleman between that environment and the main environment the facility is operating in.

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

No, the modules/subsystems are always applicable.

- 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?*

No, the system is operated only at the Albany VA Medical Center (VAMC) at this time for pilot testing. It has been approved as a national solution and will be deployed to other VAMCs moving forward.

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

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

PCSIP is not the authoritative source of PII/PHI data, this is Veterans Health Information Systems and Technology Architecture (VistA) and the SORN is:

79VA10 / 85 FR 84114, *Veterans Health Information Systems and Technology Architecture (VistA) Records–VA* (12/23/2020)
<https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>

PCSIP is provided under –Public Law 114-31; Veteran Information: Title 38, United States Code, Section 5107, Title 38, United States Code, Section 5106, and Title 38 United States Code 5701. Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I),

Version date: October 1, 2024

titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources. "Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." E-government Act of 2002 (44 U.S.C. §208(b)). 38 United States Code 5706.

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 Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

H. What is the SORN?

No SORN exists for PCSIP as it is not the authoritative source for the data. Vista is the authoritative source of data with SORN 79VA10 / 85 FR 84114, *Veterans Health Information Systems and Technology Architecture (Vista) Records-VA* (12/23/2020) <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>

I. SORN revisions/modification

No SORN exists for PCSIP as it is not the authoritative source for the data.

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

No SORN exists for PCSIP as it is not the authoritative source for the data.

4. System Changes

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

☐ Yes

☒ No

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

☐ Yes

☒ No

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Other PII/PHI data elements: Business Phone Number, Employee ID#

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.

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

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

All the patient information is read from and written to VistA. Patient Care Systems Integration Platform (PCSIP) (formerly Corey Workflow manager) reads the list of patients arrived in Emergency from Vista/EDIS or patients scheduled for surgery from VistA and pulls patient information from VistA for only the patients that are scheduled for surgery that day or are being provided care for in Emergency that day. As the patient goes thru the procedure on the day of surgery or goes through the process of care, the VA care providing staff updates timestamps on what was done for the patient at what time for patient tracking purposes. The VA staff completes the clinical documentation for the care provided to the patient in CoreyHealth™ and CoreyWebApp™, this clinical documentation of care is written by Core Mobile system to VistA as it is updated in the CoreyHealth™ or CoreyWebApp™.

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

The internal VA VistA is the authoritative source for patient data. Aside from patient data, if an unknown person or a relative of person who brings the patient to emergency may provide their name and phone number as a contact, that information is not saved to structured patient record in Vista and is discarded by PCSIP at the end of the day.

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

Yes, in the form of clinical documentation (medical record information) which is pushed back to the authoritative system in real time as the operations are performed. PCSIP also utilizes Artificial Intelligence to determine future appointment dates and post-procedure care needed.

1.3 Methods of information collection

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3 a 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?

All information is exchanged via either a standard internet browser or mobile application.

1.3 b 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 forms used for collection of information are TIU (Text Integration Utilities) notes in CPRS/Vista and 1010EZ 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.

Information is expected to be correct in the authoritative source. All existing data integrity rules and mechanisms are leveraged from VistA. The data transmission is done using Health System Seven (HL-7) protocol over TCP/IP (Transmission Control Protocol / Internet Protocol) with built-in checksum values to prevent any data corruption during transmission.

Note that the PII is only read and displayed within the system in anonymized format and de-identified. e.g. Date of Birth (DOB) is converted to Age before display.

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?

No, a commercial aggregator is not used by this system.

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

PCSIP is not the authoritative source of PII/PHI data, this is Veterans Health Information Systems and Technology Architecture (VistA) and the SORN is:

79VA10 / 85 FR 84114, *Veterans Health Information Systems and Technology Architecture (VistA) Records-VA* (12/23/2020)

<https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>

PCSIP is provided under –Public Law 114-31; Veteran Information: Title 38, United States Code, Section 5107, Title 38, United States Code, Section 5106, and Title 38 United States Code 5701. Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources. "Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." E-government Act of 2002 (44 U.S.C. §208(b)). 38 United States Code 5706.

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 information listed in the characterization of the system section 1.1 above falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

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: *The collection ties with the purpose of the underlying mission of the organization and its enabling authority.*

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

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

Principle of Data Quality and Integrity: *VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.*

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

Follow the format below when entering your risk assessment:

Privacy Risk: The privacy risk in CoreyHealth™ and CoreyWebApp™ is due to Date of Birth of patient that is read from VistA/Cerner but then converted to age and shown in the app. The risk is only when date of birth is received in the system and converted to age.

The associated risk is patient health information (PHI) being visible to someone who is not authorized to view this information. No PII is exposed.

Mitigation: The mitigation steps taken are listed below.

- (1) All information shown is in anonymized and de-identified.
- (2) The only PII received from VistA/Cerner is Date of Birth which is converted to age before displayed to end-user.
- (3) The PII received by the server is encrypted in transit and encrypted in storage in the database.

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
Name	File Identification purposes	File Identification purposes via Corey Patient mobile app
Partial Social Security Number	File Identification purposes	File Identification purposes via Corey Patient mobile app
Date of Birth	File Identification purposes	File Identification purposes via Corey Patient mobile app
Personal Mailing Address	File Identification purposes	File Identification purposes via Corey Patient mobile app
Personal Phone Number(s)	File Identification purposes	File Identification purposes via Corey Patient mobile app
Personal Email Address	File Identification purposes	File Identification purposes via Corey Patient mobile app
Business Phone Number(s)	File Identification purposes	File Identification purposes via Corey Health mobile & Web app
Business Email Address	File Identification purposes	File Identification purposes via Corey Health mobile & Web app
Employee ID#	File Identification purposes	File Identification purposes via Corey Health mobile & Web app
Emergency Contact/Next of Kin Information	Visit/Treatment purposes	File Identification purposes via Corey Patient mobile app
Sex	File Identification purposes	File Identification purposes via Corey Patient mobile app
Medications	Visit/Treatment purposes	Not used
Medical Record Number	Visit/Treatment purposes	Not used
Medical Records	Visit/Treatment 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?

PCSIP does not generate new patient data. The system generates the same data that is already being entered into VistA for each patient but does it in an easy-to-use manner from mobile devices and user interface designed and customized for specific users and backed by artificial intelligence and machine learning. This enables scheduling optimization, seamless patient tracking, and clinical documentation leading to improved efficiency, increased access to care and improved patient outcomes.

2.2 b 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 system does not create or make available new or previously unutilized information about any individuals.

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.

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

All Servers are configured and maintained with the VA Standard Image(s).

Communication is over internal VAMC networking with all information in transit and at rest encrypted per VA guidelines.

2.3 b 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).

Only the last four of the social security number is used. In addition to this truncation, the system is internal on the VA network with no public access to SSNs.

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

PII/PHI is safeguarded by:

- 1) only VA Authorized users accessing the system using multifactor authentication
- 2) the system is hosted internal to the VAMC
- 3) all communication occurring on the internal VAMC network

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?

Any VA employee involved in their department's patient treatment that day, who authenticates to the system with their VA credentials, has access to the PII.

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

Yes, however, PCSIP does not separately document criteria, procedures, controls or responsibilities as this is controlled by the VA. PCSIP does not create additional level of Authentication and Authorization. PCSIP brings forward authentication and authorization from VA's Active Directory, Multifactor Authentication, Vista and CPRS. PCSIP does document criteria, procedures, controls, or responsibilities because PCSIP leverages existing VA mechanisms which are well documented within the VA and are outside the control of PCSIP.

2.4c Does access require manager approval?

Yes, manager approval to access PCSIP is required since PCSIP leverages VA's Active Directory and Multi-factor authentication along with listing the users in the PCSIP command center for valid users of PCSIP as directed by the manager/supervisor of the user.

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

Yes, access to PCSIP is being monitored, tracked, and/or recorded.

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

PCSIP complies with all testing and assessment requirements in the VA to include code scanning and continuous monitoring. The system owner is responsible for delegating to appropriate staff for remediation of all findings. The VA is responsible for all standard images and communication channels.

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

PCSIP only retains data (PHI/PII) in the system for 24 hours, leveraging the authoritative EHR source as the repository for data. The analytics data retained in the system for analytics reports does not have PHI or PII. This results in minimization of PII as required by DM-1 and avoids the need to establish DM-2 security controls as required for Data Retention and Disposal.

3.2 How long is information retained?

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

PCSIP does not retain PII in the system for more than 24 hours.

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?

No, PCSIP does not retain PII in the system for more than 24 hours.

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

There is no retention schedule as PCSIP does not retain PII in the system for more than 24 hours. Once the patient completes the department's workflow (steps) for whatever is being done (surgery, chemotherapy/radiation, emergency discharge, labs/xrays/tests), their information is transferred to the authoritative EHR and deleted from PCSIP.

3.4 What are the procedures for the elimination or transfer of SPI?

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

The system keeps data for patients under treatment that day. Once the patient is discharged, that patients record is freed up and next patient is brought in. The new patient record is pulled in a new data structure overwriting the previous data for the patient that already went through the system.

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.

PCSIP does not use PII for testing, training, and research. Testing of system functionality is performed on VA assets with test data, also known as dummy data, which is fictional and not related to “real” individual.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a privacy risk in retaining PII/PHI in PCSIP for 24 hours for staff that is authorized to access that information. The minimal risk is associated with incidental disclosure of a VA staff speaking out the last name and someone else associating the last name with anonymized information in PCSIP.

Mitigation: All VA employees agree not to review information that they do not have a valid need-to-know to review. Staff that is not authorized in Vista/CPRS to access that information will not have access to PHI/PII. However, waiting room receptionist and the display in waiting room anonymizes the name and social security number to minimize the risk of exposure to PII.

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

4.1 a PCSIP consists of 3 (that process PII) 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 PCSIP 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
CoreyPeriop™ (aka Crystal – the main operational database)	Yes	No	<ul style="list-style-type: none">•Name•Partial Social Security Number•Date of Birth•Personal Mailing Address•Personal Phone Number(s)•Personal Email Address•Emergency Contact Information•Sex•Medical Record Number•Medical Records•Medications	File Identification and visit/treatment purposes	Encryption of Data in Transit and Data at Rest; Access Controls
CoreyMapping™ (mapping)	Yes	No	<ul style="list-style-type: none">•Name	File Identification	Encryption of Data in

between PCSIP & VistA)			<ul style="list-style-type: none"> • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact Information • Sex • Medical Record Number • Medical Records • Medications 	and visit/treatment purposes	Transit and Data at Rest; Access Controls
CoreyAnalytics™ (retrospective and predictive performance analytics)	Yes	No	<ul style="list-style-type: none"> • Name • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact Information • Sex • Medical Record Number • Medical Records • Medications 	File Identification and visit/treatment purposes	Encryption of Data in Transit and Data at Rest; Access Controls

4.1 b 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

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
Veterans Health Administration (VHA) Veterans Health Information Systems and Technology Architecture (VistA)	Identification and visit/treatment purposes	<ul style="list-style-type: none"> • Name • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact Information • Sex • Medical Record Number • Medical Records • Medications 	HTTPS/443 HL7 interface
Varian ARIA	Identification and visit/treatment purposes	<ul style="list-style-type: none"> • Name • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact Information • Sex • Medical Record Number • Medical Records • Medications 	HTTPS/443 HL7 interface
Connection between PCSIP and its minor app “CoreyHealth”,	Identification and visit/treatment purposes	<ul style="list-style-type: none"> • Name • Partial Social Security Number 	Mobile Application

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
used by VA Staff on VA devices		<ul style="list-style-type: none"> • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact Information • Sex • Medical Record Number • Medical Records • Medications 	

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: There is a privacy risk of an unauthorized user gaining access to the data.

Mitigation: The privacy risks are mitigated by:

1. Anonymizing the patient's name
2. Converting date of birth to age
3. Not using the patient's home phone number and only using the patient's mobile phone number only once to invite the patient to download and use the patient app.
4. Leveraging PIV based login to access PII only when it is needed for identification of the patient.
5. Following established staff user authentication and authorization policies for getting into the application and the accessing information from CPRS using access code/verify code or Oauth 2.0 token in Single Sign-on infrastructure.
6. Encrypting the patient information when stored and when in transit between CPRS and Core Mobile system.

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
CoreyPatient (iOS/Android) mobile application: patients/caregivers using the mobile	File Identification purposes	<ul style="list-style-type: none"> • Name • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number 	MOU/ISA	Mobile Application

app to register from their devices		<ul style="list-style-type: none"> • Personal Email Address • Sex • Emergency Contact Information 		
CoreyPatient (iOS/Android) mobile application: VA staff using the mobile app to register patients from VA devices	File Identification purposes	<ul style="list-style-type: none"> • Name • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number • Personal Email Address • Sex • Emergency Contact Information 	MOU/ISA	Mobile Application

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, but there is an externally connected mobile application, used by patients on their personal devices, that responds to reminders from the PCSIP system. The patient is sent the URL to the mobile application, along with temporary credentials, and they use the application to register themselves into PCSIP. There is a minimal risk that the URL and temporary credentials could be sent to the incorrect cellular telephone number, that would introduce the risk of displaying anonymized name through the application. There is no PII sent to the patient application.

Mitigation: Even if the incorrect individual receives the URL and temporary credentials, the verification of multi-factor variables by email and text message help reduce the improper use of the application.

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.

6.1 a 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.

PCSIP does not collect information from a patient. This is inherited from the VA within VistA. Veterans are provided a NOPP every 3 years. If a patient is brought to Emergency department by a person who provides their contact information, that information is held for the day of service and deleted after that from PCSIP. The temporarily held information is accepted in the application after providing notice to the entering user.

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

79VA10 / 85 FR 84114, *Veterans Health Information Systems and Technology Architecture (VistA) Records-VA* (12/23/2020)
<https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>

6.1 b If notice was not provided, explain why.

PCSIP does not collect information from a patient. This is inherited from the VA within VistA. Veterans are provided a NOPP every 3 years. If a patient is brought to Emergency department by a person who provides their contact information, that information is held for the day of service and deleted after that from PCSIP. Except for Emergency Contact Information, PCSIP receives all PII/PHI from the upstream system VistA for which a NoPP was provided to the individual at the time data was entered into that system. Additionally, veterans are provided with a NoPP by the VA via mail every 3 years or when there is a change to the NoPP.

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

PCSIP does not collect information from an individual. This is inherited from the VA within VistA. Veterans are provided a NOPP every 3 years.

NOPP Link:

https://dvagov.sharepoint.com/sites/vacovetsprivacy/vhapo/Documents/Guidebooks,%20Fact%20Sheets%20and%20Practice%20Briefs/NoPP_10-163_09_30_2022.pdf

79VA10 / 85 FR 84114. Veterans Health Information Systems and Technology Architecture (VistA) Records – VA <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>

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.

PCSIP does not collect information from an individual. This is inherited from the VA within VistA. Veterans are provided a NOPP every 3 years. The VHA Notice of Privacy Practice (NOPP) is a document which 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.

NOPP Link: 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.”

PIA Link: <https://department.va.gov/privacy/privacy-impact-assessments/>

Notice is provided in the SORN. The system of record (SOR) from which PII/PHI is retrieved for used in the PCSIP system is VistA. The SORN for VistA is:

79VA10 / 85 FR 84114, Veterans Health Information Systems and Technology Architecture (VistA) Records–VA (12/23/2020) <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>

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.

PCSIP does not collect information from an individual. This is inherited from the VA within VistA. Veterans are provided a NOPP every 3 years as stated in 6.1a.

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 the Emergency POC may not be made aware that their information is included in the patient record associated with the visit/treatment.

Mitigation: This risk is mitigated by the notice directly and specifically to the Emergency POC in the CoreyPatient mobile application.

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.

*7.1 a 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 \(efoia-host.com\)](https://efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

Address, Redress, and Correction would have to take place in the VA authoritative system. PCSIP does not have this capability or interaction with individuals.

7.1 b 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)?

Address, Redress, and Correction take place in the VA authoritative system, either CPRS or Cerner. This would occur at physical registration or check-in at the facility upon arrival. PCSIP does not create another point of such authentication and authorization. All Privacy Act provisions for access are conformed to by PCSIP by bringing forward the VA's authoritative system Vista/CPRS or Cerner along with Multi-factor authentication as mandated by using the PIV card.

7.1 c 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?

Address, Redress, and Correction take place in the VA authoritative system, either CPRS or Cerner. This would occur at physical registration or check-in at the facility upon arrival. PCSIP does not create another point of such authentication and authorization. All Privacy Act provisions for access are conformed to by PCSIP by bringing forward the VA's authoritative system Vista/CPRS or Cerner along with Multi-factor authentication as mandated by using the PIV card.

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.

Address, Redress, and Correction take place in the VA authoritative system, either CPRS or Cerner. This would occur at physical registration or check-in at the facility upon arrival. PCSIP does not create another point of such authentication and authorization. All Privacy Act provisions for access are conformed to by PCSIP by bringing forward the VA's authoritative system Vista/CPRS or Cerner along with multi-factor authentication as mandated by using the PIV card.

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.

Address, Redress, and Correction take place in the VA authoritative system Vista/CPRS. 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 ensure data accuracy.***

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Address, Redress, and Correction take place in the VA authoritative system.

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.

7.5 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 veterans and other members of the public will not know about the VA method for Access, Correction, Redress.

Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans are enrolled for health care and verifying information prior to receiving care. 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.

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.

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

VA Clinical staff access PCSIP through the application URL on the VA computer they are using and use their VA credential to logon. Application access is controlled by their permissions in Active Directory security groups and permissions in CPRS.

A patient (or VA employee assisting them) uses the CoreyPatient mobile application to locate themselves in the authoritative EHR and register their upcoming visit in PCSIP.

VA clinical staff also use the CoreyHealth mobile application on VA iPads/mobile devices to update treatment or process information in PCSIP.

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

There are no users from other agencies (outside the VA) who may have access to the system under any roles.

8.1 c 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.

System Administrators: use VA privileged user credentials to administer all components of the system.

VA Staff: register patients via the web app, move patients through the departmental workflow manually

Patients: register via the mobile application, send feedback messages to providers

Emergency POC: register themselves into the system via the mobile application as the person accompanying the patient.

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

Yes, by the contractors that design/maintain the system as well as any VAMC/clinical staff that are contractors.

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

The system is designed and maintained by contractor support staff.

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

Yes, the contractor, as well as any contracted providers (doctors/nurses/etc), are all required to sign confidentiality agreement.

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

Yes, the contractor that designs/maintains the system has an implemented BAA.

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

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

The contractor support staff that have gone through the VA Onboarding process, have signed NDAs, and are issued VA credentials. In addition, they have elevated privileges to the system using VA issued privileged credentials.

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.

PCSIP is accessed by Clinical Staff Users from VA provided Government Furnished Equipment (GFE) desktops/laptops, iPads, iPhones using VA provided PIV cards and PINs. These are VA employees and contractors that have gone through the background checks needed to access the patient information including anonymized form of PHI/PII.

The staff users of Core Mobile system are the same staff users that use CPRS/VistA today and have gone thru HIPAA training in the past before using the system.

The system is maintained by a contractor that has gone through similar background checks and issued PIV cards and PINs. In addition, this contractor has elevated privileges to the system using USB token and PIN. The contractor has completed the following trainings.

1. Elevated Privileges for System Access
2. Government Ethics
3. Information and Privacy Role Based Training for IT Specialists
4. Information and Privacy Role Based Training for Software Developers
5. Information and Privacy Role Based Training for System Administrators
6. Information and Privacy Role Based Training for System Owners
7. VA Privacy and Information Security Awareness and Rules of Behavior

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 01-Feb-2024
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 01-May-2024
5. *The Authorization Termination Date:* 01-May-2026
6. *The Risk Review Completion Date:* 26-Mar-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 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. (Refer to question 1.8 of the PTA)

No cloud technology is in use.

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.

There is no hosting CSP.

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.

There is no hosting CSP.

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.

There is no hosting CSP.

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 RPA is in use in PCSIP.

Section 10. References

Summary of Privacy Controls by Family


Summary of Privacy Controls by Family

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

Signature of Responsible Officials


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

**ANTHONY
BUDHRAM**

 Digitally signed by ANTHONY
BUDHRAM
Date: 2025.05.16 07:37:01 -04'00'


Privacy Officer, Anthony Budhram

**RYAN
GORDON**

 Digitally signed by RYAN
GORDON
Date: 2025.05.15 14:28:35
-04'00'

Information System Security Officer, Ryan Gordon

**RICHARD
LOUBRIEL**

 Digitally signed by RICHARD
LOUBRIEL
Date: 2025.05.16 07:45:48 -04'00'

Information System Owner, Richard Loubriel

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).

79VA10 / 85 FR 84114, *Veterans Health Information Systems and Technology Architecture (VistA) Records–VA* (12/23/2020)
<https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>

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 \(va.gov\)](#)