Privacy Impact Assessment for the VA IT System called:

Patient Care Systems Integration Program (PCSIP)

Veterans Health Administration (VHA)

Albany Stratton VAMC

eMASS ID # 1258

Date PIA submitted for review:

10/18/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Heidi DeCarlo	Heidi.Decarlo@va.gov	518-626-6944
Information System Security Officer (ISSO)	Kurt Olendorf	Kurt.Olendorf@va.gov	518-626-6242
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?".

Patient Care Systems Integration Program (PCSIP) provides multiple facility departments (Emergency, Surgery, 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.

It 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) and other EHRs including Cerner and EPIC.

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 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 Care Systems Integration Program (PCSIP); Albany Stratton VAMC

B. *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 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.

C. *Who is the owner or control of the IT system or project?*

VA Owned and VA 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?*

PCSIP leverages Vista as the system of record and stores information only for patients that are current under care at a specific department. For example, Emergency Department at Albany VAMC may have anywhere between 1 and 30 patients at any time. 30 number of individuals whose information is stored in PCSIP. In surgery, there may be 20 cases scheduled in a day, PCSIP will hold 20 patients' information. The typical individual is an emergency, surgical or ICU patient as well as provider(s). The patient information is only in PCSIP for 24 hours before being transferred via VistA to Computerized Patient Record System (CPRS) as the authoritative Electronic Health Record (EHR) source of the data.

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

The patient information that is anonymized and then accessed by VA staff after multi-factor authentication and authorization includes, patient's current complaint, patient surgery schedule, patient demographics, vitals, allergies, immunizations, past medical history, surgery prep instructions, discharge instructions, orders and consults

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

Patient information is pulled via VistA from CPRS for processing, and pushed back via VistA to CPRS for permanent inclusion into the patients' medical record in the EHR.

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 only at the Albany VAMC at this time but is designed to be an Enterprise solution for use in multiple areas.

3. Legal Authority and SORN

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

PCSIP is not the authoritative source of PII/PHI data. Patient information is pulled from CPRS for processing, and pushed back to CPRS for inclusion into the patient EHR when the patient is done with care in emergency, surgery, radiology or wards.

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?*

No SORN exists

4. System Changes

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

PCSIP is customized to existing workflows and business processes in emergency, surgery, radiology, wards so completion of this PIA will not require changes in business processes.

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

Completion of this PIA will not result in technology changes because PCSIP still keeps Vista as the system of record and all components of PCSIP run on VA baselined servers and VA provided devices.

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
□ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity
□ Tax Identification Number

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

☒ Medical Record Number
☒ Gender
☐ Integrated Control Number (ICN)

☐ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

VISN#, Facility ID, Floor#, Room#, Visit/appointment information, multiple Date/Time elements (checkins/outs, starts/ends, etc), date of death (where applicable), clinic stop code, Provider information (Name, ID, Role), Procedure information (Name/Type, etc), System Operational fields (IDs, Status, Connector, Send Attempts, Error Codes, etc), Username/Password, User Country/State.

PII Mapping of Components (Database)

PCSIP consists of 4 database instances. 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 3.9 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
CoreyMirth Database™ instance	No	Yes	All identified: Name, SSN, DoB, Gender, Race, Addresses, Phones	Channels, configuration and data processing parser	Transparent Data Encryption (TDE) plus field level encryption
CoreyPeriop (Crystal) Database instance	No	Yes	All identified: Name, SSN, DoB, Gender, Race, Addresses, Phones	Patient Identification and tracking	Transparent Data Encryption (TDE) plus field level encryption
CoreyMapping Database instance	No	Yes	All identified: Name, SSN, DoB, Gender, Race, Addresses, Phones	Data element mapping between PCSIP and VistA	Transparent Data Encryption (TDE) plus

					field level encryption
CoreyAnalytics Database instance	No	Yes	All identified: Name, SSN, DoB, Gender, Race, Addresses, Phones	System performance retrospective & predictive analytics and reporting	Transparent Data Encryption (TDE) plus field level encryption

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?

All the patient information is read from and written to VistA. Patient Care Systems Integration Program (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 ED 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™, these forms or clinical documentation of care is written by Core Mobile system to VistA as it is updated in the CoreyHealth™ or CoreyWebApp™.

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

The internal VA CPRS (and Vista) is the authoritative source for patient data.

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

PCSIP information is pushed back to the internal VA CPRS system in real time as the operations are performed.

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?

All information is exchanged with CPRS via VistA using Health System Seven (HL-7) protocol and Kernel Installation and Distribution System (KIDS) builds installed on VistA servers after review and acceptance by Field Enhancement & Sustainment Interface & Quality Assurance (QA) Division at VA (Frank O'Brian, Cheryl Fashandi et al).

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

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.

Information is expected to be correct in CPRS. All existing data integrity rules and mechanisms are leveraged from CPRS/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 in the app in anonymized format and de-identified. E.g. Date of Birth (DOB) is converted to Age before display in app.

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

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

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.

PCSIP is covered under VA SORN (System of Records Notice) # 79VA10A7 – Veterans Health Information Systems and Technology Architecture (VistA) Records-VA.

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.

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: The privacy risk in CoreyHealth™ and CoreyWebApp™ is due to Date of Birth of patient that is read from CPRS 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 due to 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 CPRS is Date of Birth which is converted to age before display 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	Not used
Date of Birth	File Identification purposes	Not used
Gender	File Identification purposes	Not used
Email Address	File Identification purposes	Not used
Mobile Phone number	File Identification purposes	Not used

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?

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.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing *record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.*

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

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?

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.

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

Only the last four of the social security number is used. Two factor authentication is used to access information within the system. (PIV).

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

Only VA Authorized users access the system using multifactor authentication, the system is hosted internal to the VAMC, and communication is via internal VAMC networking.

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

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

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

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

<u>Principle of Use Limitation:</u> 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?

PCSIP does not display PII to end-users. PCSIP follows the Fair Information Practice Principles currently followed by VA's VistA and CPRS by enabling staff to continue to use existing FIPPs while enabling increased efficiency, access to care and improved outcomes. The authentication of users is done using PIV card, authorization is done using VistA established mechanisms of access code & verify code and the privacy of information is ascertained by anonymizing PII and de-identifying information per established VHA guidelines and confirmed via software source code by VHA Software Assurance team.

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

Yes, both in PCSIP documentation as well as in the GRC tool Enterprise Mission Assurance Support System (eMASS)

2.4c Does access require manager approval?

Yes, access requires the use of the VA Personal Identity Verification (PIV) card, and in order to acquire a PIV, the holder must go through the VA process for obtaining their PIV.

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

Yes, the OS of each server creates the required system logs for monitoring/tracking/recording.

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

PCSIP complies with all testing and assessment requirements in the VA, to include code scanning and continuous monitoring. The vendor is responsible for mitigating 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 does not retain patient data (PHI/PII) in the system but instead leverages CPRS as the repository of retention of patient data. The analytics data retained in the system for analytics reports does not have PHI or PII. This results in minimization of PII and avoids the need to establish DM-2 controls.

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.*

PCSIP does not retain PII in the system.

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?
PCSIP does not retain PII in the system.

3.3b Please indicate each records retention schedule, series, and disposition authority?
PCSIP does not retain PII in the system.

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 patient 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 thru 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. All the testing is performed on VA provided test Vista with scrambled data.

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: The privacy risk is non-existent due to anonymization of all PHI/PII and holding the anonymized PHI/PII for the period of day of surgery only when this anonymized PHI/PII is accessed by the care providers. Once anonymized, there is no PII in PCSIP.

Mitigation: There is no privacy risk hence does not require mitigation. The risk is avoided by anonymizing the PHI/PII and holding it for period of 1 day only during day of surgery or while patient is in emergency department. Once anonymized, there is no PII in PCSIP.

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 CPRS via VistA	Patient Health Information for VA staff to provide care.	• Last Name • First Name (or Initial) • Phone Number • Last 4 of SSN • Date of Birth • Gender • Email Address	Electronically pulled from CPRS using HL- 7 and Mumps code delivered via KIDS build after anonymization / de- identification

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is	***List the purpose of information being shared /***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement,***	***List the method of transmission and the measures in***

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

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

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

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

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

Follow the format below:

<u>Privacy Risk:</u> Not applicable – PCSIP is an internal system

<u>Mitigation:</u> None

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.

PCSIP does not collect information from an individual. This is inherited from the VA within CPRS. 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

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

PCSIP does not collect information from an individual. This is inherited from the VA within CPRS. 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

6.1c 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.

PCSIP does not collect information from an individual. This is inherited from the VA within CPRS. 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 CPRS. 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

6.3 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 CPRS. 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

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: There is a risk that veterans and other members of the public will not know that an Area/VA Medical Center exists or that it collects, maintains, and/or disseminates PII, PHI or PII/PHI about them

Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans are enrolled for health care. s. 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.

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.***

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

7.1b 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)?

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

7.1c 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?

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

7.2 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 would have to take place in the VA authoritative system. PCSIP does not have this capability or interaction with individuals.

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

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.

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

7.5 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 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. 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.

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?

The VA staff users access the system using PIV card and PIN in compliance with VA policies.

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

There are no users from other agencies.

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.

Patients: Register via the mobile apps, send feedback messages to providers
VA Staff: Register patients via the web app, move patients through the departmental workflow manually
System Administrators: use VA privileged user credentials to administer all components of the system.
The VA staff users access the system using PIV card and PIN in compliance with VA policies.

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.

PCSIP is accessed by Clinical Staff Users from VA provided GFE desktops/laptops, iPads, iPhones using VA provided PIV cards and PIN. 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 system is maintained by contractor support staff that have gone through the VA Onboarding process and signed NDAs. They are issued PIV card and PIN. In addition, the support contractors have elevated privileges to the system using USB token and PIN.

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 GFE desktops/laptops, iPads, iPhones using VA provided PIV cards and PIN. The se 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 card and PIN. 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 Has Authorization and Accreditation (A&A) been completed for the system? Yes

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 25-Aug-2023
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 05-May-2023
5. *The Authorization Termination Date:* 01-Nov-2023
6. *The Risk Review Completion Date:* 26-Apr-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.***
N/A

Section 9 – Technology Usage

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

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?
If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.
Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

No, cloud technology is not in use.

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.*

N/A

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.

N/A

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.

N/A

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).

N/A

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.

Heidi DeCarlo
533588

Digitally signed by Heidi DeCarlo
533588
Date: 2023.11.28 15:09:13 -05'00'

Privacy Officer, Heidi DeCarlo

KURT
OLENDORF

Digitally signed by KURT
OLENDORF
Date: 2023.11.28 15:20:22
-05'00'

Information System Security Officer, Kurt Olendorf

RICHARD
LOUBRIEL

Digitally signed by RICHARD
LOUBRIEL
Date: 2023.11.28 16:52:03 -05'00'

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).

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