Privacy Impact Assessment for the VA IT System called:

Consolidated Mail Outpatient Pharmacy (CMOP) Pharmaceutical System (major application)

Leavenworth Consolidated Mail Outpatient Pharmacy (CMOP) (1305) (minor application); Chelmsford Consolidated Mail Outpatient Pharmacy (CMOP) (1299) (minor application); Tucson Consolidated Mail Outpatient Pharmacy (CMOP) (1306) (minor application); Dallas Consolidated Mail Outpatient Pharmacy (CMOP) (1300) (minor application); Murfreesboro Consolidated Mail Outpatient Pharmacy (CMOP) (1303) (minor application); Great Lakes Consolidated Mail Outpatient Pharmacy (CMOP) (1304) (minor application); Charleston Consolidated Mail Outpatient Pharmacy (CMOP) (1298) (minor application)

Veterans Health Administration

Consolidated Mail Outpatient Pharmacy (CMOP)

eMASS ID #1307 and minor applications

Date PIA submitted for review:

8/15/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Courtney D. Albritton	Courtney.albritton@va.gov	913-928-9202
Information System Security Officer (ISSO)	Anna J. Johnson	Anna.johnson3@va.gov	575-693-8320
Information System Owner	John Koveos	John.koveos@va.gov	978-435-1533

Abstract

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

The Consolidated Mail Outpatient Pharmacy (CMOP) Local Area Network (LAN), Veterans Health Information System Technology Architecture (VistA) and Cerner are used to transfer, process, manage, and update the prescription data received from VA Medical Centers (VAMCs) throughout the automated prescription fulfillment distribution workflow.

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?

The Consolidated Mail Outpatient Pharmacy (CMOP) Pharmaceutical System (CPS), VHA Consolidated Mail Outpatient Pharmacy (CMOP)

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

The CMOP Pharmaceutical System (CPS) receives prescription batch transmissions from all VAMC VistA servers through the CMOP VistA and Cerner Servers. The prescription batch transmissions are then downloaded from the VA VistA System and Cerner System to the CPS via flat file transfer using Health Level 7 (HL7) protocol and SQL databases respectively. The CPS interacts with the VAMCs and CMOP production systems to provide functionality by balancing the workloads to ensure timely prescription processing. CPS receives and processes data from all VAMCs and Indian Health Services (IHS).

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

The CMOP is VA owned and VA operated. It is an office under VA End User Services (EUS), Infrastructure Operations (IO), Application Services, Operations Control

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?

The CMOP accurately fills and ships over 117,000,000 prescriptions per year for healthcare beneficiaries including our nation's Veterans, active-duty service members, and patients eligible for care through IHS. The CMOP also has agreements with the Department of Defense (DoD) and the Direct to Patient (DTP) partners Medline and McKesson to provide prescription and pre-packaged medical supply fulfillment.

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

One of the CMOP's missions in the Department of Veterans Affairs (VA) is to maintain and manage its automated pharmaceutical prescription filling systems per The Joint Commission Comprehensive Accreditation Manual for Home Care. The CMOP uses multiple complex automated pharmaceutical prescription filling systems which employ a mixture of highly automated robotic devices, conveyor systems, and human factors.

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

Cerner and other partners provide the CMOP services for management of prescriptions throughout the lifecycle of the prescription that allow a single prescription to be filled locally or by the CMOP, and allows Veterans, providers, and the local VA pharmacies to change, track, and monitor CMOP prescriptions. This includes bi-directional communications between the Electronic Health Record (EHR) and designated Regional CMOPs, accounting for sending and receiving patient and prescription data. After Regional CMOPS and Direct to Patient (DTP) vendors send packages, the CPS consolidates tracking information and provides that to My Healthy Vet (MHV) so patients can track prescription status.

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?*

CPS, the major application, supports/receives support from the seven regional CMOPs, the minor applications. All PII collected is encrypted at rest and in transit, and the same controls are used at each location.

3. Legal Authority and SORN

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

https://www.oprm.va.gov/privacy/systems_of_records.aspx

Patient Medical Record – VA (24VA10A7/85FR62405)

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

The SORN will not require amendment or revision and approval at this time.

4. System Changes

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

No

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

No

Section 1. Characterization of the Information

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

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

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

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

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
□ Medical Record Number
□ Gender
□ Integrated Control Number (ICN)
□ Military History/Service Connection
□ Next of Kin
□ **X** Other Data Elements (list below)

Other PII/PHI data elements: RX Number, quantity ordered, instructions for use, physician's name, prescribing VAMC name, VAMC address and VAMC telephone number.

PII Mapping of Components (Servers/Database)

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

The CMOP systems consist of one major application (CPS) and seven minor applications which are housed at the individual CMOP Regional facilities. All CMOP systems have been analyzed to determine if Personally Identifiable Information (PII) is collected. The type of PII collected and the reasons for the collection of the PII are in the table below. The prescription data is entered into the patient's pharmacy records at the VAMC of care. It is then transmitted to the CMOP via Health level 7 (HL7) protocol through Mailman, a VistA data transfer feature. CMOP fulfills the prescription order using our automated pharmaceutical dispensing systems. CMOP then transmits back to the VAMC of care information concerning the medication dispensed (Date Dispensed, National Drug Code (NDC), Lot Number, Expiration Date)**.** The reasons for the collection of the PII are in the table below.

CPS and the regional CMOPs consist of approximately 288 servers and 111 databases. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CPS and the regional CMOPs and the reasons for the collection of the PII are in the table below.

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**
VISTA	Yes	Yes	Patient's name, address, SSN, RX Number, type of medication, quantity ordered, instructions for use, physician's name, prescribing VAMC name, address and telephone number	Prescription Fulfillment	VA Gold Image, Patched, with all VA required security controls in place
My Healthevet (MHV)	Yes	Yes	Patient SSN, Patient Name, Patient Address (mailing and home address), Patient Phone Number, Patient Account Number, Prescribing Doctor, Medication Prescribed, Prescription Directions, Last time Medication was refilled, When the Prescription Expires.	Patient Notification, Package Tracking	VA Gold Image, Patched, with all VA required security controls in place

Cerner	Yes	Yes	Patient SSN, PatientName, Patient Address (mailing address and home address), Patient Phone Number, Patient Account Number, Prescribing Doctor, Medication Prescribed, Prescription Directions, Last time Medication was refilled, When the prescription expires	Prescription Fulfillment	VA Gold Image, Patched, with all VA required security controls in place
CMOP Web Servers	Yes	Yes	Patient SSN, Patient Name, Patient Address (mailing address and home address), Patient Phone Number, Patient Account Number, Prescribing Doctor, Medication Prescribed, Prescription Directions, Last time Medication was refilled, When the prescription expires	Prescription Fulfillment	VA Gold Image, Patched with all VA required security controls in place
CMOP Database Servers	Yes	Yes	Patient SSN, Patient Name, Patient Address (mailing address and home address), Patient Phone Number, Patient Account Number, Prescribing Doctor, Medication Prescribed, Prescription Directions, Last time Medication was refilled, When the prescription expires.	Prescription Fulfillment	VA Gold Image, Patched with all VA required security controls in place
CMOP Application Servers	Yes	Yes	Patient SSN, Patient Name, Patient Address (mailing address and home address), Patient Phone Number, Patient Account Number, Prescribing Doctor, Medication Prescribed, Prescription Directions, Last time Medication	Prescription Fulfillment	VA Gold Image, Patched, with all VA required security controls in place

			was refilled, When the prescription expires		

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?

The prescription data is entered into the patient's pharmacy records at the VAMC of care. It is then transmitted to the CMOP via HL7 protocol through Mailman, a VistA data transfer feature. CMOP will fulfill the prescription order using our automated pharmaceutical dispensing systems. CMOP then transmits back to the VAMC of care information concerning the medication dispensed (Date Dispensed, NDC, Lot Number, Expiration Date).

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 prescription information is collected directly from the attending physician or medical staff at the VAMC of care or IHS. It is then electronically transmitted to the CMOP via HL7 protocol through VistTA messaging. VistA software has been developed by VA and is used to support clinical and administrative functions at VAMC's nationwide.

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

CPS does not create scores, analysis, or reports.

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?

As stated previously, prescription information is collected directly from the attending physician or medical staff at the VAMC of care or IHS. It is then electronically transmitted to the CMOP via HL7 protocol through VistTA messaging. The use of VistA software has been mandated by VA to support clinical and administrative functions at VAMC's nationwide.

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 CMOP does not use forms to collect information.

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.

The VAMC is responsible for the accuracy of the data transmitted to CMOP. Accuracy is verified by the original source. HL7 protocol is used for the transmission to CMOP ensuring that the data sent is the data received. Data is not manipulated at the CMOP and is processed as it is received. CMOP further verifies the physical contents of the packages we send out to ensure that all data elements including the prescription label and the medication dispensed are consistent.

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

The CMOP does not use a commercial aggregator.

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

SORN 24VA10P2

Legal authority can be found in the following US Code: Title 5 United States Code, section 301 and Title 38, United States Code, Sections 109, 111, 501, 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728 and 7105 and Title 38, United States Code, Section 7301; Executive Order 9397. Title 38, United States Code, Sections 501(b) and 304. Records maintained at the VA Health Care Facility to include pharmaceutical subsidiary record information which the CMOP provides back to the VAMC as part of the patient's records.

Additional information about state laws, and local policies.

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

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*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: There is a privacy risk that data within the patient record may be inaccurate due to its reliance on manual input by Medical Center staff.

Mitigation: The VAMC is responsible for the accuracy of the data transmitted to CMOP. Accuracy is verified by the original source. HL7 protocol is used for the transmission to CMOP ensuring that the data sent is the data received. Data is not manipulated at the CMOP and is processed as it is received. We are responsible for ensuring the prescriptions are filled correctly based on the data sent and reviewed for accuracy by a pharmacist.

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	To identify Veteran	Not used
Social Security Number:	Identifier at the VAMC of care (not used at the CMOP)	Not used
Mailing Address	To identify where to mail the prescriptions	Not used
Zip Code	To identify where to mail the prescriptions	Not used

Phone Number	Received as part of the transmission from the Medical Center (not used at the CMOP)	Not used
Current Medications	Identifies medications to be filled and processed by CMOP	Not used
RX Number	To identify the RX	Not used
Quantity Ordered	Quantity of medication to dispense per RX	Not used
Instructions for Use	Instructions from the physician on use of RX	Not used
Physician's Name	Prescribing physician	Not used
Prescribing VAMC name, VAMC Address and VAMC telephone number	Prescribing VAMC information	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?
The CPS and CMOP LANs are used to manage the prescription data received from the VAMC of care to fulfill the order and mail it to the patient. There is no additional data analysis performed.

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.
Filling information is added to the existing record and exported back to the Medical Center to show date/time prescription is filled, NDC, lot number and expiration date. Quality Assurance reviews are conducted on the data and performance measures are calculated monthly.

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?
The entire database containing the patient information is encrypted.

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

The entire database containing the patient information is encrypted.

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

The prescription data is entered into the patient's pharmacy records at the VAMC of care. It is then transmitted to the CMOP via HL7 protocol through Mailman, a VistA data transfer feature. CMOP will fulfill the prescription order using our automated pharmaceutical dispensing systems. CMOP then transmits back to the VAMC of care information concerning the medication dispensed (Date Dispensed, NDC, Lot Number, Expiration Date). The entire database containing the patient information and the connections to and from the database are encrypted.

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?

All CMOP employees must take VA Privacy and Information Security Awareness Training and read and acknowledge the Rules of Behavior (ROB) annually, as well as taking Privacy and HIPAA focused training.

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

Yes. Access to the systems is based on the requirements of the position (pharmacists, pharmacy technicians, packers, OIT, administrative staff, etc.) and is documented both in TMS and in local records.

2.4c Does access require manager approval?

Yes. Supervisors determine the level of access needed and assign functional categories when employees are on-boarded, then review annually at a minimum.

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

Yes. Auditing and accountability are done through Windows Authentication. Also, if personnel are delinquent in their annual training requirements, their accounts are flagged for immediate remediation or removal from the network.

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

All personnel are responsible for safeguarding PII.

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

Pharmaceutical records to include name, social security number, mailing address, zip code, medication type, medication quantity, instructions for use, instructions from the physician on use of RX, prescribing physician, prescribing VAMC name, prescribing VAMC Address and prescribing VAMC telephone number.

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.*

CMOP records are purged from the LAN Production Systems every 45 days. The data is maintained in the CPS server for 6 months then transferred to the Archive Server where records are purged in accordance with the Record Control Schedule (RCS) 10-1 for Pharmacy records. Data is then purged from the CPS server.

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?

Yes

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

RCS 10-1 VHA Records Control Schedule (RCS 10-1), Chapter 6, 6000.1d (N1-15-91-6, Item 1d) and 6000.2b (N1-15-02-3, Item 3).

RCS 10-2 http://www.va.gov/vhapublications/rcs10/rcs10-1.pdfRecords Control Schedule 10-1 (va.gov)

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

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

Paper records are shredded by a shredding company. CMOP has Business Associate Agreements (BAAs) with National Association Information Destruction (NAID) eligible data destruction vendors who supply on-or off-site destruction per the contract. Certificates of destruction are required that state date and number of materials destroyed. System data is purged through an automated purge set by the RCS 10-1 for pharmacy records. http://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdfRecords Control Schedule 10-1 (va.gov)

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

No research is done at CMOP. All testing data meets the VA Displaying Sensitive Data Guidelines to remove referencing SSNs in any written material or test databases containing patient data. The Social Security Administration (SSA) has indicated that SSNs beginning with the series 000 or 666 should be used as display numbers. These series have not and likely never will be issued as valid SSNs. We use the following format for referencing patient names anywhere sensitive patient/staff data may be displayed. The patient's name shall be constructed from the abbreviated application name concatenated with "patient" for the last name and the use of textual numbers or a numeric for the first name. An alpha character or numeric can be added to the last name to make it more distinctive in recognizing specific test entities (e.g., CMOP patient, One; CMOPpatient2, One; CMOPpatientA, One; CMOP patient, 12). Addresses and phone numbers are scrambled. The provider's name is constructed from the abbreviated application name concatenated with "provider" for the last name, and the use of textual numbers or a numeric for the first name. An alpha character or number can be added to the last name to make it more distinctive in recognizing specific test entities. (e.g., CMOPprovider, One; CMOPprovider1, One; CMOPproviderB, One; CMOPprovider, 12). Training material is reviewed by the Privacy Officer (PO) to ensure no PII is in the material. The presenter must obtain a signed VA0897 from the PO prior to providing training to staff without the need to know. The signer certifies that all materials used in the presentation, including PowerPoint files, handouts, or other presentation documentation complies with privacy guidelines regarding protection of PII.

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 associated with this system is that CMOP may retain the information for longer than necessary to fulfill CMOP's mission.

Mitigation: CMOP records are purged from the LAN Production Systems every 45 days. The data is maintained in the CPS server for 6 months then transferred to the Archive Server where records are purged in accordance with the Record Control Schedule (RCS) 10-1 for Pharmacy records. Data is then purged from the CPS server. All pharmacy data is maintained in the patient's records at the VAMC of record.

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?

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***
Vista	Health Care	Veteran's pharmaceutical prescription information is temporarily retained. Information includes Patient's name, address, SSN, RX number, type of medication, quantity ordered, instructions for use, physician's name, prescribing VAMC name, address and telephone number. Patient identifiers are purged from the VISTA system after data is received by the production systems and prescription has been filled	Internal connection to VA infrastructure via VISTA, which uses SFTP to transfer HL7 files
My Healthevet (MHV)	Health Care	Veteran's pharmaceutical prescription information is temporarily retained. Information includes Patient's name, address, SSN,	Internal connection to VA infrastructure

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***
		RX number, type of medication, quantity ordered, instructions for use, physician's name, prescribing VAMC name, address, and telephone number. Patient identifiers are purged from the VISTA system after data is received by the production systems and prescription has been filled.	via VISTA, which uses SFTP to transfer HL7 files
Cerner	Health Care	Veteran's pharmaceutical prescription information is temporarily retained. Information includes Patient's name, address, SSN, RX number, type of medication, quantity ordered, instructions for use, physician's name, prescribing VAMC name, address, and telephone number. Patient identifiers are purged from the VISTA system after data is received by the production systems and prescription has been filled.	Internal connection to VA infrastructure via VISTA, which uses SFTP to transfer HL7 files
Consolidated Mail Outpatient Pharmacy (CMOP) Web Servers, Database Servers, and Application Servers	Health Care	Patient SSN, Patient Name, Patient Address (mailing address and home address), Patient Phone Number, Patient Account Number, Prescribing Doctor, Medication Prescribed, Prescription Directions, Last time Medication was refilled, When the prescription expires	Internal connections to VA Infrastructure

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The privacy risk associated with this system is that CMOP could inappropriately use or disclose information, either intentionally or unintentionally.

Mitigation: CMOP mitigates this privacy risk by requiring all users to complete Security and Privacy Awareness Training, which includes appropriate and inappropriate uses and disclosures of the information accessible to them as part of their official duties. User activity in the system is monitored and audited. Should a user inappropriately use or disclose information, he or she is subject to loss of access and the disclosure will be referred to the appropriate internal investigation entities. Information is not shared outside of CMOP as part of normal agency operations. Information may be shared from the source systems from the VAMC of care, pursuant to published Routine Uses outlined in 24VA10P2 Legal Authority—Title 38,United States Code, Sections 501(b) and 304.

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.

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?

***Note: All external connections are made at the major application, CPS. All documents supporting these external connections (i.e. MOU/ISAs) are maintained under CPS in eMASS.*

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Medline Pharmaceutical	Prescription fulfillment	Patient SSN, Patient Name, Patient Address (mailing address and home address), Patient Phone Number, Patient Account Number, Prescribing Doctor, Medication Prescribed, Prescription Directions, Last time Medication was refilled, when the prescription expires.	MOU/ISA	VPN Site to Site
McKesson Pharmaceutical	Prescription fulfillment	Patient SSN, Patient Name, Patient Address (mailing address and home address), Patient Phone Number, Patient Account Number, Prescribing Doctor, Medication Prescribed, Prescription Directions, Last time Medication was refilled, When the prescription expires.	MOU/ISA	VPN Site to Site
Federal Express Supply Chain, Inc. (FSC)	Mail Consolidation	Patient SSN, Patient Name, Patient Address (mailing address and home address), Patient Phone Number, Patient Account Number, Prescribing Doctor, Medication	MOU/ISA	SFTP

		Prescribed, Prescription Directions, Last time Medication was refilled, When the prescription expires.		

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: The privacy risk associated with this system is that CMOP could inappropriately use or disclose information, either intentionally or unintentionally.

Mitigation: CMOP mitigates this privacy risk by requiring all users to complete security and privacy awareness training, which includes appropriate and inappropriate uses and disclosures of the information accessible to them as part of their official duties. User activity in the system is monitored and audited. Should a user inappropriately use or disclose information, he or she is subject to loss of access and the disclosure will be referred to the appropriate internal investigation entities. Information is not shared outside of CMOP as part of normal agency operations. Information may be shared from the source systems from the VAMC of care, pursuant to published Routine Uses outlined in 24VA10P2 Legal Authority—Title 38, United States Code, Sections 501(b) and 304.

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.
This is the responsibility of the Medical Center of care. Additional notice is provided through the Notice of Privacy Practices (NOPP) VHA Forms and Publications - Publications - Brochures (va.gov) and Privacy Impact Assessment (PIA) which is available online as required by the eGovernment Act of 2002, Pub.L.107-347 § 208(b)(1)(B)(iii), the Department of Veterans Affairs, and the following VA Systems of Record Notices (SORNs) which are published in the Federal Register and available online: SORN title: Patient Medical Records-VA (24VA10A7/85FR62405) https://www.oprm.va.gov/privacy/systems of records.aspx

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.
CMOP Pharmaceutical System (CPS). This is the responsibility of the Medical Center of care.

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.
This is the responsibility of the Medical Center of care. Please see attached NoPP. VHA Forms and Publications – Publications – Brochures (va.gov)

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.
Individuals can decline to provide information without a penalty except for the means test process. Non-service-connected Veterans and Veterans who are in receipt of a service-connected compensation of less than 50% may decline to give a financial assessment called a means test and as a result, may be placed in category 8 and billed for certain services. This is the responsibility of the VAMC of Care. Individuals are provided with a copy of IB 10-163, Notice of Privacy Practices, by the Medical Center of record upon verbal or written request. All Veterans receive a copy of this notice from the Health Eligibility Center (HEC) upon enrollment.

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.
Veterans may utilize the 10-5345 (Request for Authorization to Release Medical Records or Information) to state with whom his/her information may be shared. This is done through the VAMC of Record. Veterans have the right to opt in or opt out of the VAMC facility directory. This is done at the VAMC of Record.

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: The privacy risk associated with this system is that the individual will not have prior or existing notice of data collection and uses of information after collection by the source system.

Mitigation: Individuals are provided with a copy of IB 10-163, Notice of Privacy Practices, by the VAMC of Record upon verbal or written request. All Veterans receive a copy of this notice from the Health Eligibility Center (HEC) upon enrollment.
PIAs and SORNs are both notices. SORN title: Patient Medical Records-VA (24VA10A7/85FR62405
https://www.oprm.va.gov/privacy/systems of records.aspx

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.***

All CMOP Freedom of Information Act (FOIA) requests are directed to the VHA FOIA Office. CMOP would provide information requested to the VAMC or VHA FOIA for dissemination. The VAMC of Care holds responsibility for individuals to gain access to their information since they are the primary system of record. When requesting access to one's own records, patients are asked to complete VA Form 10-5345a 9 (Individual's Request for a Copy of their Own Health Information) which can be obtained from the VAMC or online at https://www.va.gov/vaforms/medical/pdf/VHA Form 10-5345a Fill-revision.pdf

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)?

This system is exempt from the access provisions of the Privacy Act. It is the responsibility of the Medical Center of care.

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?

Additionally, Veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the MyHealthevet program which is VA's online personal health record. More information regarding MyHealthevet may be found at https://myhealth.va.gov/index.html. In addition to the procedures discussed above, SORN: Patient Medical Records-VA (24VA10A7) http://www.oprm.va.gov/privacy/systems_of_records.aspx addresses record access.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are provided the opportunity to submit a request for change in a medical record via the amendment process. An amendment is the authorized alteration of health information by modification, correction, addition, or deletion. An individual may request an alteration to their health information by making a formal, written request mailed or delivered to the VA health care facility that maintains the record. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. A request for amendment of information contained in a system of records will be processed by the PO. In reviewing requests to amend or correct records, the PO must be guided by the criteria set forth in VA regulation 38 CFR 1.579. VA must maintain in its records only such information about an individual that is accurate, complete, timely, relevant, and necessary.

Individuals have the right to review and change their contact or demographic information at time of appointment or upon arrival at the VA facility and/or submit a change of address request form to the VAMC of Care Business Office for processing.

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.

Verbal inquiries regarding the amendment request process are generally received by the VAMC of Care Business Office, Release of Information Office, Patient Experience Officer, or PO. Inquiries regarding the amendment request process can be explained by any member of the VAMC of Care, Release of Information Office, Patient Experience Officer, or the PO. The amendment process is also explained in the Notice of Privacy Practices (NOPP). Individuals are provided with a copy of IB 10-163, Notice of Privacy Practices, by the VAMC of Record upon verbal or written request. All Veterans receive a copy of this notice from the HEC upon enrollment.

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.

The VAMC of Care PO provides appeal rights to the Office of General Counsel or VHA Privacy Office via the written response to the Veteran regarding the outcome of the amendment request.

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: The privacy risk associated with this system is that patients will not have the ability to assess or correct their information once it is at the CMOP. This must be done prior to transmitting the information to CMOP at the VAMC of Care.

Mitigation: The CMOP CPS and LANs are merely conduits for the information maintained at the VAMC. We do not change or manipulate the data we receive. The VAMC can request that we cancel back a prescription to them prior to dispensing so they can alter the data. Information related to access, redress, and correction can also be found in the applicable SORN: http://www.oprm.va.gov/privacy/systems of records.aspx

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

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

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

8.1a Describe the process by which an individual receives access to the system?
Access is restricted to VA employees who must complete both the HIPAA and Information Security training. Specified access is granted based on the employee's functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information System Security Officers (ISSOs), Facility Chief Information Officers (FCIOs), System Administrators (SAs), Network Administrators (NAs), Database Managers (DMs), users of VA information systems or VA sensitive information. Access is requested utilizing Enterprise Service Desk (ESD) procedures. Electronic Permission Access System (ePAS) is used for elevated privileges.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?
Users from the VA, contractors, and outside agencies/vendors may have access to the system. Users submit access requests based on need to know and job duties. These requests are submitted for VA employees, contractors and all outside agencies/vendors and are processed through the appropriate approval processes. Once access is granted, individuals can log into the system(s) through dual authentication, i.e., a Personal Identity Verification (PIV) card with a PIN. Once inside the system, individuals are authorized to access information on a need-to-know basis.

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.

Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked however specifics on how this is done can be found in the program office PTA and PIA.

Access to computer rooms is generally limited by appropriate locking devices and restricted to authorized VA employees and vendor personnel. Automated Data Processing (ADP) peripheral devices are placed in secure areas (areas that are locked or have limited access) or are otherwise protected. Information that is downloaded from VistA and maintained on laptops and other approved government equipment is afforded similar storage and access protections as the data that is maintained in the original files. Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes. Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection at the health care facility, or an OIG office location remote from the health care facility, is controlled in the same manner. Information downloaded from VistA and maintained by the OIG headquarters and Field Offices on automated storage media is secured in storage areas for facilities to which only OIG staff have access. Paper documents are similarly secured. Access to paper documents and information on automated storage media is limited to OIG employees who have a need for the information in the performance of their official duties. Access to information stored on automated storage media is controlled by individually unique passwords/codes.

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.

Certain contractors have been granted access to the CPS and CMOP LANs. Access is necessary to fulfill their contract. Security clearances are required as well as VA Security and Privacy Training. The following training is required at onboarding and annually via the VA Talent Management System (TMS): (1) Information Security and Privacy Awareness and Rules of Behavior; and (2) Privacy and HIPAA training must also be completed if access to PHI. Contracts and access are reviewed annually. BAAs are obtained on contracts for which it is determined one is needed.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

All VA employees who have access to VA computers must complete the onboarding and annual mandatory privacy and information security training. In addition, all employees who have access to PHI must complete the VHA mandated Privacy and HIPAA Focused training. The PO, ISSO, and IT staff also perform subject specific training on an as needed basis.

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

8.4a If Yes, provide:

1. *The Security Plan Status: Current through 3/25/2025*
2. *The System Security Plan Status Date: 01/12/2022*
3. *The Authorization Status: Full Authority to Operate (ATO)*
4. *The Authorization Date:* 03/25/2022
5. *The Authorization Termination Date: 3/25/2025*
6. *The Risk Review Completion Date:* 07/28/2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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.

Yes. CPS uses the Amazon Web Services Government Private Cloud and Microsoft Azure Government for disaster recovery.

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.*

Not applicable

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.

Not applicable

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.

Not applicable

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

The role of BOTS is to process prescriptions.

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 provided in this Privacy Impact Assessment is true and accurate.

COURTNEY ALBRITTON

Digitally signed by COURTNEY ALBRITTON
Date: 2024.10.29 14:06:41 -04'00'

Privacy Officer, Courtney D. Albritton

ANNA JOHNSON

Digitally signed by ANNA JOHNSON
Date: 2024.10.29 09:24:56 -07'00'

Information Systems Security Officer, Anna J. Johnson

JOHN KOVEOS

Digitally signed by JOHN KOVEOS
Date: 2024.11.01 11:04:51 -04'00'

Information Systems Owner, John Koveos

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