Privacy Impact Assessment for the VA IT System called:

VistA Pharmacy Controlled Substances

Assessing

Veterans Health Administration (VHA)

PCS Patient Care Services

eMASS ID #1050

Date PIA submitted for review:

May 17, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Dennis Lahl	Dennis.lahl@va.gov	202-461-7330
Information System Security Officer (ISSO)	Richard Alomar-Loubriel	richard.alomar-loubriel@va.gov	787-696-4091
Information System Owner	Dena Liston	Dena.Liston@va.gov	304-886-7367

Abstract

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

VistA - Pharmacy: Controlled Substances Assessing is an internal system to the VA service hosted by the VA Enterprise Cloud (VAEC) using Amazon Web Services (AWS) Platform as a service (PaaS), for use by VistA systems. It will allow Pharmacy Benefits Management personnel to share up-to-date Controlled Substance Provider information so that providers with expired Drug Enforcement Agency (DEA) credentials cannot prescribe Controlled Substances for VA. Updated Provider information is uploaded to the web service by Pharmacy Benefits Management personnel on a periodic basis and stored in the VAEC AWS Elastic File System. This file is parsed by the web service and made available for querying by VistA systems in a system-to-system integration.

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?

VistA - Pharmacy: Controlled Substances Assessing (Pharm-CS) is owned by the program office of PCS Patient Care Services. The project is under control of The Office of Information Technology (OIT) DevSecOps (DSO) Software Product Management (SPM) – Health.

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 business purpose of Pharmacy Controlled Substances Web Service (Pharm-CS) is to allow Pharmacy Benefits Management personnel to share Controlled Substance Provider information so that providers with expired DEA credentials cannot prescribe Controlled Substances for VA.

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

The Pharmacy Controlled Substances Web Service (Pharm-CS) is owned by the program office of PCS Patient Care Services. The project is under control of The Office of Information Technology (OIT) DevSecOps (DSO) Software Product Management (SPM) – Health.

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 downloaded file includes every provider who can prescribe controlled medication. There are approximately 2 million providers in the file.

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

The Pharmacy: Controlled Substances Web Service (Pharm-CS) is an internal to the VA service hosted by the VA Enterprise Cloud (VAEC) using Amazon Web Services (AWS) Platform as a service (PaaS), for use by VistA systems. It will allow Pharmacy Benefits Management personnel to share up-to-date Controlled Substance Provider information so that providers with expired DEA credentials cannot prescribe Controlled Substances for VA. Updated Provider information is uploaded to the web service by Pharmacy Benefits Management personnel on a periodic basis and stored in the VAEC AWS Elastic File System. This file is parsed by the web service and made available for querying by VistA systems in a system-to-system integration.

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

The DEA file uploaded to the web service by Pharmacy Benefits Management personnel on a periodic basis and stored in the VAEC AWS Elastic File System. The DEA file is parsed by the DEA Lookup web service and made available for querying by VistA systems in a system-to-system integration. The data is not shared with any other system or individual.

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?

N/A; Pharm-CS is an Enterprise application.

3. Legal Authority and SORN

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

The following are citations of the legal authority to operate the IT system.

• HIPAA (Public Law 104-191) : Health Insurance Portability and Accountability Act of 1996

• 38 USC 8111 : Sharing Of Department Of Veterans Affairs And Department Of Defense Health Care Resources

• USC 1104 : Purposes And Authority Of Center

• 25 USC Sections 1645 : Sharing arrangements with Federal agencies

• 25 USC Sections 1647 : Eligible Indian Veteran Services

• 38 USC Sections 523(a) : Coordination And Promotion Of Other Programs Affecting Veterans And Their Dependents

• 38 USC Sections 6301 : Purpose; Definitions

• 38 USC Sections 6302 : Veterans' Benefits

• 38 USC Sections 6303 : Biennial Plan

• 38 USC Sections 6304 : Veterans Assistance Offices

- 38 USC Sections 6305 : Out Stationing Of Counseling And Outreach Personnel
- 38 USC Sections 6306 : Use Of Other Agencies
- 38 USC Sections 6307 : Outreach For Eligible Dependents
- 38 USC Sections 8153 : Sharing Of Health-Care Resources
- 38 USC 8153 : Sharing Of Health-Care Resources

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

The system is not in the process of being modified and the existing SORN does not require amendment or revision.

4. System Changes

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

NO

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

NO

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name
☐ Social Security Number
☐ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☐ Personal Phone Number(s)
☐ Personal Fax Number
☐ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers
☒ Certificate/License numbers[1] (DEA registration number)
☐ 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
☒ Other Data Elements (list below)
- Business activity code
- Business activity subcode

Other PII/PHI data elements: <<Add Additional Information Collected but Not Listed Above Here (For Example, A Personal Phone Number That Is Used as A Business Number)>>

PII Mapping of Components (Servers/Database)

<**VistA – Pharmacy: Controlled Substances Assessing**> consists of <**1** key component (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by <**VistA – Pharmacy: Controlled Substances Assessing**> 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,	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

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

Application Program Interface (API) etc.) that contains PII/PHI					
DEA Lookup service (DEALS)	**No, the file is provided by DOJ**	**Yes**	**DEA Registration Number, Name, Address, City, State, Zip Code**	**Pharmacy Benefits Management personnel to share Controlled Substance Provider information so that providers with expired DEA credentials cannot prescribe Controlled Substances for VA.**	**File is stored in 2 factor authenticated system.**

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?

Updated Provider information is uploaded to the web service by Pharmacy Benefits Management personnel on a periodic basis and stored in the VAEC AWS Elastic File System. This file is parsed by the web service and made available for querying by VistA systems in a system-to-system integration. The uploaded file is saved to an encrypted filesystem assessable to the Service.

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 DOJ is the system of record for the Pharm-CS webservice.>>

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

<< Updated Provider information is uploaded to the web service by Pharmacy Benefits Management personnel on a periodic basis and stored in the VAEC AWS Elastic File System. This file is parsed by the web service and made available for querying by VistA systems in a system-to-system integration.>>

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?

Updated Provider information is uploaded to the web service by Pharmacy Benefits Management personnel on a periodic basis and stored in the VAEC AWS Elastic File System. This file is parsed by the web service and made available for querying by VistA systems in a system-to-system integration.

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?

N/A because this system does not collect any data/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.

If the file transmits correctly from the DOJ, it is assumed to be accurate. The file that resides in the cloud service is not validated with any checksum.

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?

<< If the file transmits correctly from the DOJ, it is assumed to be accurate. The file that resides in the cloud service is not validated with any checksum.>>

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

site6 (https://www.oprm.va.gov/privacy/systems_of_records.aspx).
173VA005OP2 / 86 FR 61852 "VA Enterprise Cloud-Mobile Application Platform (Cloud) Assessing (VAEC-MAP" https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf . Authority for Maintenance of the system is found in Title 38, United States Code, section 7301(a).

- HIPAA (Public Law 104-191): Health Insurance Portability and Accountability Act of 1996
- 38 USC 8111: Sharing Of Department Of Veterans Affairs And Department Of Defense Health Care Resources
- USC 1104: Purposes And Authority Of Center
- 25 USC Sections 1645: Sharing arrangements with Federal agencies
- 25 USC Sections 1647: Eligible Indian Veteran Services
- 38 USC Sections 523(a): Coordination And Promotion Of Other Programs Affecting Veterans And Their Dependents
- 38 USC Sections 6301: Purpose; Definitions
- 38 USC Sections 6302: Veterans' Benefits
- 38 USC Sections 6303: Biennial Plan
- 38 USC Sections 6304: Veterans Assistance Offices
- 38 USC Sections 6305: Out Stationing Of Counseling And Outreach Personnel
- 38 USC Sections 6306: Use Of Other Agencies
- 38 USC Sections 6307: Outreach For Eligible Dependents
- 38 USC Sections 8153: Sharing Of Health-Care Resources
- 38 USC 8153: Sharing Of Health-Care Resources

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:

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

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

<u>Principle of Individual Participation:</u> 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: PII personal data of medical providers could be exposed during breach.

Mitigation:

- VA Enterprise and AWS architecture in adherence to information security policies make the risk of breach of data extremely low. The system does not collect any data. PBM uploads a file obtained from DEA. The data from this file is used by VistA to identify providers who can prescribe controlled substances.
- Pharm-CS adheres to information security requirements instituted by the VA Office of Information Technology (OIT) and the VA Enterprise Cloud (VAEC) Program.
- Pharm-CS System Categorization Level is Moderate, and the data is stored in a FedRAMP certified High environment protected by High level security controls.
- Both contractor and VA employees are required to take Privacy, Health Insurance Portability and Accountability Act (HIPAA), and information security training annually.
- Pharm-CS access is granted only to Role Holders with a need to access the data.

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.

It will allow Pharmacy Benefits Management personnel to share up-to-date Controlled Substance Provider information so that providers with expired DEA credentials cannot prescribe Controlled Substances for VA

PII/PHI Data Element	Internal Use	External Use
<< • Name • Personal Mailing Address • Business activity code	File Identification purposes	Not used

• Business activity subcode • DEA Registration Number >>		

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 DEALS system provides an access mechanism for administrative data. The data is managed by Pharmacy Benefits Management (PBM) and is periodically uploaded to the DEALS system manually by PBM personal. DEALS is not an authoritative system. It is a replica of the PBM data used to provide VistA access to the data. DEALS does not collect new data, or otherwise manipulate the data it receives from PBM.

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 DEALS system provides an access mechanism for administrative data. The data is managed by PBM and is periodically uploaded to the DEALS system manually by PBM personal. DEALS is not an authoritative system. It is a replica of the PBM data used to provide VistA access to the data. DEALS does not collect new data, or otherwise manipulate the data it receives from PBM.>>

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 Pharm-CS system utilizes the VAEC administered AWS FedRAMP cloud platform. All at-rest data is encrypted. All data transmissions are encrypted via TLC 1.2 HTTPS.

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

Not Applicable. VistA Pharm-CS does not process or retain Social Security Numbers.

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

The Pharm-CS system utilizes the VAEC administered AWS FedRAMP cloud platform. All at-rest data is encrypted. All data transmissions are encrypted via TLC 1.2 HTTPS.

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?

<<This is handled by username and password>>

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

<<Access information is documented with in the Pharm-CS Access Control (AC) Standard Operating Procedure (SOP). >>

2.4c Does access require manager approval?

<<N/A there is no individual user access to this information. There is no user level access to the system>>

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

<<Pharm-CS does not track the access to this information the only account that can access information is a System Account.>>

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

<<Safeguards are inherited by VA AWS.>>

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

DEA Registration Number, Business Activity Code, Name, Personal Mailing Address, and Business Activity Sub-Code. There is no database. The copy of the DEA file is refreshed by the Pharmacy user.

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.*

The DEA provider file is stored indefinably. The DEA file is refreshed periodically by the Pharmacy user. The old file is overwritten when the new file is uploaded by PBM.
The system follows the retention plan as noted in the SORN - NARA General Records Schedules GRS 20, item 1c and GRS 24, item 6a.

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?

The DEA provider file is stored indefinably. The DEA file is refreshed periodically by the Pharmacy user. The old file is overwritten when the new file is uploaded by PBM.
The system follows the retention plan as noted in the SORN - NARA General Records Schedules GRS 20, item 1c and GRS 24,
item 6a.

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

NARA General Records Schedules GRS 20, item 1c and GRS 24, item 6a.

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 DEA provider file is stored indefinably. The DEA file is refreshed periodically by the Pharmacy user. The old file is overwritten when the new file is uploaded by PBM.
The system follows the retention plan as noted in the SORN - NARA General Records Schedules GRS 20, item 1c and GRS 24, item 6a.

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.
The system does not utilize PII for research.

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: If information is retained longer than specified, privacy information may be released to unauthorized individuals.

Mitigation: The data is transient to the system and is refreshed in VistA. The temporary data is stored in an encrypted file system in the cloud. In addition, all data at rest within the Pharm-CS security boundary is encrypted in accordance with FIPS 140 2, as well as protected by EDRAMP certified "High" security controls.

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.

The purpose of the information being shared is to facilitate identification of clinical resources.

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 (VHA) under Pharmacy Benefits Management (PBM)	DEA Lookup Service (DEALS)	Name, Personal Mailing address, DEA number, expiration date, business activity code. Business activity subcode	FIPS 140-2 Encrypted TCP

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 risk associated with Internal sharing is unauthorized disclosure.

Mitigation: Users of the system are required to take TMS training pertinent to their general role at the VA. This includes understanding HIPAA and rules of behavior. Access in VA is limited to authorized users.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A – Not shared externally	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: There is no external sharing.

Mitigation: There is no external sharing.

Section 6. Notice

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

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

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

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

Yes, a notice is provided. SORN: VA Mobile Application Environment (MAE)-VA" (173VA005OP2), Document Number: 2021–24368.

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

https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.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.

The DEALS system provides an access mechanism for administrative data. The data is managed by PBM and is periodically uploaded to the DEALS system manually by PBM personal. DEALS is not an authoritative system. It is a replica of the PBM data used to provide VistA access to the data. DEALS does not collect new data, or otherwise manipulate the data it

receives from PBM. In other words, Pharm-cs does not collect or maintain the data/information. It only serves as a mechanism to get the data from PBM to VistA.

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.

Yes, they can decline to obtain a DEA license to prescribe controlled substances. The provider will be unable to prescribe controlled medications if they are not on the DEA list. If they are not on the list the Pharmacist will not fill the prescription.

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.

The process occurs outside the DEALS. Pharmacist consent to review and update of their credentials to fill controlled substance as required by Federal law. There is no PHI collected. The provider exercises consent for use of PII when requesting a DEA number from the DOJ application.

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

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

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

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

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

<u>Privacy Risk:</u> It is not VA responsibility to give notice to the collection of the DEA credential information. DOJ collects that information and provides VA access to it. Access to DEALS is limited by username and password protection.

Mitigation: The Pharmacist receives mandatory HIPAA and Security training to minimize risk of improper use and disclosure.

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.***

This is not applicable as Pharm-CS does not have knowledge of the procedure the DOJ has in place that allow access to information.

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

The DEALS system provides an access mechanism for administrative data. The data is managed by PBM and is periodically uploaded to the DEALS system manually by PBM personal. DEALS is not an authoritative system. It is a replica of the PBM data used to provide VistA access to the data. DEALS does not collect new data, or otherwise manipulate the data it receives from PBM. There is a formal agreement between PBM and DEA called the Drug Enforcement Administration Data User Agreement which can be found in eMASS as evidence.

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?

<<The DEALS system provides an access mechanism for administrative data. The data is managed by PBM and is periodically uploaded to the DEALS system manually by PBM personal. DEALS is not an authoritative system. It is a replica of the PBM data used to provide VistA access to the data. DEALS does not collect new data, or otherwise manipulate the data it receives from PBM. There is a formal agreement between PBM and DEA called the Drug Enforcement Administration Data User Agreement which can be found in eMASS as evidence.>>

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.

The DEA file is owned and maintained by the DEA, outside the scope of Pharm-CS and the VA The data is periodically refreshed by downloading the DEA file from the DOJ.

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.

The VA does not correct information in the DEA file. The information in the file is assumed to be accurate when downloaded from the DOJ.

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 VA does not correct information in the DEA file. The provider would need to contact the DOJ if any correction was needed.

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: An individual may want to review the content of their record to check for data accuracy. The magnitude of harm associated with this risk to the VA is low because DEALS is not the authoritative source of the data. The system does not collect any data. PBM uploads a file obtained from DEA. The data from this file is used by VistA to identify providers who can prescribe controlled substances. VAEC–MAP uses the VAEC AWS cloud environment to provide an automated platform and pipeline for the development and hosting of production VA mobile applications.

Mitigation: N/A. All participating providers are under agreement with the DOJ.

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 Web Service is authenticated through username and password. This client systems use PIV or 2FA authentication.

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?

Pharmacist will have access to PII that include contractors, non-contractors, and government employees.

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.

<<The Web Service is authenticated through username and password. This client systems use PIV or 2FA authentication. The web service maintains two roles; one allows updating the data and the other allows reading the data.

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.

Pharmacist will have access to PII that include contractors, non-contractors and government employees. Users of the Web Service are required to have signed NDAs and mandatory security training. All personnel will be required to complete all necessary on-boarding information, paperwork, and training. Developers do not have access to PII.

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 must complete annual Privacy and Security training. This training includes, but is not limited to, the following courses:

- VA 10176: Privacy and Info Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training
- VA 3812493: Annual Government Ethics

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* August 7, 2023
3. *The Authorization Status:* One (1) year ATO
4. *The Authorization Date:* November 22, 2023
5. *The Authorization Termination Date:* October 24, 2024
6. *The Risk Review Completion Date:* October 24, 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)*

The Web Service is hosted on AWS Cloud as Platform as a service (PaaS)

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.*

AWS GovCloud FedRAMP approved

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.

AWS GovCloud FedRAMP approved.

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.

DENNIS LAHL Digitally signed by DENNIS LAHL
Date: 2024.07.11 13:50:10 -04'00'

Privacy Officer, Dennis Lahl

RICHARD ALOMAR-LOUBRIEL Digitally signed by RICHARD ALOMAR-LOUBRIEL
Date: 2024.07.11 14:20:41 -04'00'

Information System Security Officer, Richard Alomar-Loubriel

DENA LISTON Digitally signed by DENA LISTON
Date: 2024.07.11 15:03:09 -04'00'

Information System Owner, Dena Liston

APPENDIX A-6.1

https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf

HELPFUL LINKS:

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

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

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

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

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices