Privacy Impact Assessment for the VA IT System called:

Pharmacy Reengineering Inbound ePrescribing Assessing (ERX-IE)

Veteran Health Administration Office

Enterprise Program Management Office

eMASS ID # 165

Date PIA submitted for review:

11/03/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	Marlene Moore	Marlene.Moore@va.gov	405-456-4673
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?".

The Pharmacy Reengineering (PRE) Inbound ePrescribing project includes the capability to receive inbound electronic prescriptions (eRxs) coming from external entities, process them, and dispense them at Department of Veterans Affairs (VA) pharmacies. It also includes the ability to electronically transfer prescriptions to other pharmacies and electronically receive transferred prescriptions from other VA and non-VA pharmacies.

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?

Pharmacy Reengineering Inbound ePrescribing Assessing (ERX-IE) - Enterprise Program Management Office

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

Inbound ePrescribing is needed to increase patient safety through the reduction of translation/transcription errors; provide process efficiencies to prescribers, patients, and pharmacies; and provide capabilities on-par with retail pharmacies, all for VA to fulfill its goal of delivering world-class, excellent healthcare to its beneficiaries. It supports the VA's Fiscal Year (FY) 2014- 2020 Strategic Plan's strategic goals to Enhance and Develop Trusted Partnerships and Manage and Improve VA Operations to Deliver Seamless and Integrated Support.

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

2. Information Collection and Sharing

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

Approximately 2,500 Veterans pharmacy order information.

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

ERX-IE primarily facilitates processing of prescription orders for pharmacy fulfillment.

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

Information is processed from providers to be shared with VA affiliated pharmacies. There are no subsystems within ERX-IE.

G. Is the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?

The application itself is centrally deployed at Austin Information Technology Center (AITC)and all respective data stored in the application schema at AITC. All patient data however does exist in the VistA accounts at each respective VAMC.

3. Legal Authority and SORN

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

SORN 79VA10 / 85 FR 84114 "Veterans Health Information Systems and Technology Architecture (VistA) Records – VA" https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. Authority for maintenance of the system: Title 38, United States Code, section 7301(a).

SORN 121VA10 / 88 FR 22112 "National Patient Databases-VA" https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf. Authority for maintenance of the system: 38 U.S.C 501.

SORN 147VA10 / 86 FR 46090 "Enrollment and Eligibility Records-VA" https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf. Authority for maintenance of the system: Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

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 SORNs will not require any amendment or revision. ERX-IE does not use cloud technology.

4. System Changes

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

The completion of this PIA will not result in circumstances that require changes to business processes.

K. Will the completion of this PIA could potentially result in technology changes?
The completion of this PIA will not result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☒ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☒ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☒ Certificate/License numbers[1]*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Medications
- ☒ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Gender
- ☐ Integrated Control Number (ICN)
- ☐Military History/Service Connection
- ☐ Next of Kin
- ☐ Other Data Elements (list below)

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

*Specify type of Certificate or License Number –
National Provider Identifier (NPI), National Council for Prescription Drug Programs (NCPDP) ID State License Number, Drug Enforcement Agency (DEA)number – Required and maintained in the ERX-IE message.

PII Mapping of Components (Servers/Database)

Pharmacy Reengineering Inbound ePrescribing Assessing consists of one key component, Oracle 19c Database SID IEPP. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Pharmacy Reengineering Inbound ePrescribing 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, 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**
Oracle 19c Database SID IEPP	Yes	Yes	Patient Internal Entry Number (IEN), Name, Date of Birth (DOB), Mailing Address, Zip Code, Phone Number (s), Email Address, Health Insurance Beneficiary Numbers Account numbers, Certificate/License numbers, Current Medications, Previous Medical Records, Gender and possibly Social Security Number (SSN) to be used for Patient Match in Master Person Index (MPI).	Oracle database is used as an intermediate storage area for messages in transit (e.g., for message processing and validation) and retains data for reporting purposes.	Elevated privileges required for access to data; approved through ePAS 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?

Electronic prescription requests are received from an external prescriber via an ePrescribing clearinghouse, Change Healthcare, and routed to a VA Pharmacy through the VA secure network.

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.

ERX-IE utilizes external prescribers as they are the only legal authorities to send this type of information through Change Healthcare.

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

The ERX-IE system does not create information in any form.

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?

Electronic prescription requests are received from an external prescriber via an ePrescribing clearinghouse, Change Healthcare, and routed to a VA Pharmacy through the VA secure network.

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?

ERX-IE does not collect information on a form and is not subject to the Paperwork Reduction Act.

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 eRx hub include automatic validations of provider information, patient information Master Person Index (MPI), enrollment & eligibility information (E&E) prior to transmitting each prescription to VistA in real time. Pharmacists working at sites use the VistA Holding Queue application to validate each prescription manually prior to filling at the VA pharmacy.

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?

ERX-IE does not check for accuracy by accessing a commercial aggregator of information.

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

Inbound ePrescribing requires and maintains certification with the clearinghouse, Change Healthcare, for authority to process prescription data.

The legal authority to operate this system is found in:

SORN 79VA10 / 85 FR 84114 "Veterans Health Information Systems and Technology Architecture (VistA) Records – VA" https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. Authority for maintenance of the system: Title 38, United States Code, section 7301(a).

SORN 121VA10 / 88 FR 22112 "National Patient Databases-VA" https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf. Authority for maintenance of the system: 38 U.S.C 501.

SORN 147VA10 / 86 FR 46090 "Enrollment and Eligibility Records-VA" https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf. Authority for maintenance of the system: Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The system stores sensitive patient information. There is a risk that information may be accessed by an unauthorized party.

Mitigation: Two-factor authentication is used to prevent unauthorized access to the system. Additionally, access to the system is only available to authorized personnel with access to the VA intranet. There is no public access to the system.

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	Used to identify the patient (i.e., Veteran or employee).	Not used
Social Security Number	Used as official patient (i.e., Veteran or employee) identifier.	Not used

Date of Birth	Used to identify the patient (i.e., Veteran or employee) and determine age of patient.	Not used
Mailing Address	Used to communicate with patient (i.e., Veteran or employee).	Not used
Zip Code	Used to communicate with patient (i.e., Veteran or employee)	Not used
Phone Number(s)	Used to communicate with patient (i.e., Veteran or employee).	Not used
Email Address	Used to communicate with patient (i.e., Veteran or employee)	Not used
Health Insurance Beneficiary Numbers Account numbers	Used for patient (i.e., Veteran or employee) billing and cost recovery.	Not used
Certificate/License numbers	Used for external provider credentialing	Not used
Current Medications	Used for healthcare & prescribing medicine.	Not used
Previous Medical Records	Used for continuity of care related to previously prescribed medicine; The information is used to route and fill prescriptions incoming to VA pharmacies from external providers.	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 Inbound eRx GUI implements a reporting feature for data analysis. However, information contained in the reports has been de-identified in accordance with VHA Directive 1605.01. Additionally, the Track/Audit feature allows authorized personnel to view information on each transaction. The transaction data does contain sensitive information; however, access is controlled by means of role-based permissions.

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.

ERX-IE does not create or make available new or previously unutilized information about an individual.

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?

Data in transit is protected by means of industry standard encryption protocols (e.g., HTTPS, VPN, etc.). Data at rest (Netapp storage array) is FIPS 140-2 compliant and fully encrypted at aggregate-level.

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

SSNs are optional attributes on inbound electronic prescriptions and may be used for identifying patient enrollment in the Master Person Index (MPI) system if provided by a non-VA provider. SSNs collected are encrypted, and the collection of that data and maintaining the system are authorized and protected by Title 38, United States Code (U.S.C.), Sections 501(b) and 304 for medical records.

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

The Office of Management and Budget (OMB) Memorandum M-06-15 is inherited by the VA Rules of Behavior (ROB) per VA Handbook 6500. The following items adhere to the directives outlined in OMB Memorandum M-06-15 and M-06-16.

Technical Safeguards:

- Two-factor authentication is used to prevent unauthorized access to the system.
- Access to the system is only available to authorized personnel with access to the VA intranet.
    - There is no public access to the system.
    - Application administrators manually add authorized users to the system and configure their role-based access permissions.
    - Timeout: Application GUI has a Session Lock configuration implemented.
    - There are no computer readable sensitive data extracts from point 4 on -16.

Administrative Safeguards:

- Electronic Permission Access System (ePAS), managed through Office of Information and Technology (OI&T), is an electronic document routing system. ePAS is used primarily for electronic access requests but capable of routing other types of documents such as:
    - Data Warehouse Access Requests
    - Medical Center Memorandum (MCM) Approvals
    - Standard User Access Request Forms
    - Web Content Requests

Physical Safeguards

- AITC supplies the facility and accompanying safeguards that are associated with housing the information system.

System Access:

- The system is only accessed through VA Intranet by means of Government Funded Equipment (GFE) laptops, Citrix Access Gateway (CAG), VA workstations. All three means of access are subject to standard VA encryption.

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?

Access to PII is determined by role-based access permissions within the eRx GUI and VistA security keys. The web-based system is integrated with SSOi for PIV-based two-factor authentication.

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

Training procedures are reviewed to ensure all VA employees are familiar with the requirements of the Privacy Act, VA's implementing regulations, and any special requirements of their specific jobs. Note: VA Directive 6502, VA Enterprise Privacy Program, provides more details on the design, development, delivery, and monitoring of privacy training for VA employees. VA employees are required to report any potential privacy violations or breaches to their ISO and Privacy Officer, and these reports are processed pursuant to VA Handbook 6500.2, Management of Security and Privacy Incidents. In addition, pursuant to the Privacy Act, the Department will review annually, the circumstances and actions of VA employees that resulted in VA being found civilly liable under Section (g) of the Privacy Act, or an employee being found criminally liable under the provisions of Section (i) of the Privacy Act. The purpose of this review is to determine the problem and find the most effective way to prevent recurrence.

2.4c Does access require manager approval?

Yes, user access requires manager approval.

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

The VA provides monitoring and tracking through SSOi.

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

All VA users per the ROB are responsible for assuring safeguards for 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*

Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Phone Number(s), Personal Fax Number, Personal Email Address, Health Insurance Beneficiary Numbers Account Numbers, Certificate/License Numbers, Current Medications, Previous Medical Records

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.*

There is no known length of retention in the application database for inbound and outbound messages. The sensitive patient information retention would be the responsibility of the end points of the message transfers, and those end points (VistA Pharmacies and Change Health Care).

The prescription record retention may be governed by Pharmacy Service in VHA Record Control Schedule (RCS)10-1 item 7400.11 Prescription File. The disposition instructions are “Temporary: Destroy after 3 years.”

For the purpose of Inbound eRx, VistA is the system of record. SORN 79VA10 ‘‘Veterans Health Information Systems and Technology Architecture (VistA) Records-VA’’ records are retained under RCS 10–1 item 2000.2 Information Technology

Operations and Maintenance Records destroy 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.

Records that fall under SORN 121VA10 ‘‘National Patient DatabasesVA’’are retained under the NARA General Records Schedule (GRS) 5.2, item 020. The disposition instructions are” Temporary: Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later.”

Records that fall under SORN 147VA10 “Enrollment and Eligibility Records-VA” are retained under RCS 10–1 items 1250.1, 1250.2 and 1250.3. For 1250.1, destroy 7 years after the income year for which the means test verification was conducted, when all phases of Veteran’s appeal rights have ended. If an appeal is filed, retain record until all phases of the appeal have ended; 1250.2, destroy 30 days after the data has been validated as being a true copy of the original data; and 1250.3, destroy when no longer needed.

RCS 10-1: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf
GRS 5.2: https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf

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?

All records are stored in accordance with the records control schedules listed in question 3.2 above.

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

Per VHA Directive 6300, the Federal Records retention requirements are enforced using RCS 10-1 and the General Records Schedule (GRS). The reporting requirements are contained in NARA Regulations (36 CFR, Part 1230 and VA handbook 6300.1. Ch.6).

The prescription record retention may be governed by Pharmacy Service in VHA Record Control Schedule (RCS)10-1 item 7400.11 Prescription File. The disposition authority is NN-166-175.

For the purpose of Inbound eRx, VistA is the system of record. SORN 79VA10 ‘‘Veterans Health Information Systems and Technology Architecture (VistA) Records-

VA'' records are retained under RCS 10–1 item 2000.2 with disposition authority DAA-GRS2013-0005- 0004, item 020.

Records that fall under SORN 121VA10 ''National Patient DatabasesVA''are retained under the NARA General Records Schedule (GRS) 5.2, item 020 (disposition authority DAA-GRS2022-0009-0002).

Records that fall under SORN 147VA10 "Enrollment and Eligibility Records-VA" are retained under RCS 10–1 items 1250.1 (disposition authority DAA-0015- 2018-0001, item 0001), 1250.2 (disposition authority DAA-0015- 2018-0001, item 0002), and 1250.3 (DAA-0015- 2018-0001, item 0003).

RCS 10-1: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.
https://www.va.gov/vapubs/search_action.cfm?dType=1

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.

PII is only used for testing in approved upper environments protected by associated security protocols for access to the information. i.e., Preproduction environment is the only lower environment approved to host PII for testing, and the VA ePAS system is utilized to restrict access to approved users.

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 system only stores sensitive patient information in the form of audited message traffic. There is no known length of retention in the application database for inbound and outbound messages. The sensitive patient information retention would be the responsibility of the end points of the message transfers, and those end points (VistA Pharmacies and Change Health Care) follow the VHA policy, 75 years after last care received. The risk is in revealing this information to an unauthorized party.

Mitigation: Two-factor authentication is used to prevent unauthorized access to the system. Additionally, access to the system is only available to authorized personnel with access to the VA intranet. There is no public access to the system.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Health Administration - Veterans Health Information System and Technology Architecture (VistA)	To perform pharmacy fulfillment.	System Log files, sample clinical data that may contain Protected Health Information (PHI)	Electronically pulled from VistA through Computerized Patient Record System (CPRS).
Department of Veterans Affairs Master Person Index (MPI)	To identify the patient.	Name, Social Security Number, Date of Birth, Sex/Gender, Mother's Maiden Name, Multiple Birth Indication, Place of Birth (City and State), SSN Verification Status, Pseudo SSN	Site to site encrypted with TLS 1.2
Veterans Health Administration Eligibility and Enrollment (E&E)	To identify the patient.	Veterans Patient Identification (VPID)	Web Service Secure electronic transmission via Transmission Control Protocol (TCP) Hypertext Transfer

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*
			Protocol Secure (HTTPS)

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: Potential loss of information could occur due to theft or destruction of data in transmission or at rest.

Mitigation: Monitors and audits are conducted to ensure security of information. Policies and procedures are in place for guidance on internal sharing and disclosure of information, along with ongoing education in privacy, security, and records management.

Sustainment is not aware of any specific risks related to sharing information within the department. The protocols for the information shared are well defined with respect to the associated systems.

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				

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: N/A as no information is share with external providers.

Mitigation: N/A as no information is share with external providers.

Section 6. Notice

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

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

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

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

The VHA Notice of Privacy Practices provides information to a patient (i.e., Veteran) on VHA's authority to share their health information without authorization for purposes of treatment (i.e., filling prescriptions)A copy of the VHA Notice of Privacy Practices is found here: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946.

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

SORN 121VA10 / 88 FR 22112 "National Patient Databases-VA" https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

SORN 147VA10 / 86 FR 46090 "Enrollment and Eligibility Records-VA" https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

This Privacy Impact Assessment (PIA) also serves as notice as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

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

Notice is provided as described in 6.1a above.

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 VHA Notice of Privacy Practices provides information to a patient (i.e., Veteran) on VHA's authority to share their health information without authorization for purposes of treatment (i.e., filling prescriptions)A copy of the VHA Notice of Privacy Practices is found here - https://vaww.va.gov/vhapublications/index.cfm

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

SORN 121VA10 / 88 FR 22112 "National Patient Databases-VA" https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

SORN 147VA10 / 86 FR 46090 "Enrollment and Eligibility Records-VA" https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

This Privacy Impact Assessment (PIA) also serves as notice as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

Information is used, accessed, and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR. Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed, and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

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 risk associated with insufficient notice is that the patient is not aware of how their PII/PHI is being used and shared.

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware

of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records. The NOPP is also available at all VHA medical centers from the facility Privacy Officer. The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

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

Prescription records processed by Inbound eRx become part of the patient's health record within VistA. There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office.
VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access.VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

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

ERX-IE is not exempt from the access provisions of the Privacy Act.

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 information in ERX-IE is maintained in a Privacy Act system.

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

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

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

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) which states:

Right to Request Amendment of Health Information.
You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.

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

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

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

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

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Formal redress via the amendment process is available to all individuals, as stated in questions 7.1-7.3

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: The risk of incorrect information in an individual's records is mitigated by authenticating information when possible. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.

The NOPP discusses the process for requesting an amendment to one's records.

The*]* Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information.
The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

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

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

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

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

> Two-factor authentication is used to prevent unauthorized access to the system. Additionally, access to the system is only available to authorized personnel with access to the VA intranet. There is no public access to the system. Application administrators manually add authorized users to the system and configure their role-based access permissions.

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

> There are no users from other agencies who may have access to ERX.

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.

> Roles specified in 8.1b are application users only and confined to the UI application for eRx. Roles in management of the database, application server, and application code is separate and standard for VA application project teams (e.g., DBAs, Java Developers, DevOps, etc).

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.

VA contractors that have access to the computer system are only delegated VistA keys and menu functions needed to complete their duty task. They are required to complete annual Privacy, Security, and Rules of Behavior training. Contractors having access to PHI/PII are required to have a Business Associate Agreement (BAA) (nationally with VHA or locally with facility). Contracts are reviewed on an annual basis by the Contracting Officer Representative (COR). The Privacy Officer and Information Security Officer monitor that the annual Privacy, Security, and Rules of Behavior training is completed by contractors and business associates. Any local BAAs are monitored by Privacy Officer to ensure compliance with HIPAA. National BAAs are monitored by the VHA Privacy Office. VA contractors under contract to perform system development and test system activities shall use redacted test patient data. No PII/PHI data is used in development or test systems. Only to development and test systems using redacted test patient data. No PII/PHI data. Only authorized contractor personnel with elevated privilege are granted access to production data.

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.

Annual role-based training for system administrators is mandated for all personnel with elevated privileges. Annual privacy training is administered through the VA Talent Management System (TMS) system.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* 5/26/2023
2. *The System Security Plan Status Date:* Complete expires 5/26/2024.
3. *The Authorization Status:* Authority to Operate (ATO)
4. *The Authorization Date:* 7/12/2023
5. *The Authorization Termination Date:* 7/11/2024
6. *The Risk Review Completion Date:* 6/14/2023
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.***

Section 9 – Technology Usage

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

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

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

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

No, the system does not use cloud technology.

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

No, the system does not use cloud technology.

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

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

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

No, the system does not use cloud technology.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

No, the system does not use cloud technology.

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

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

No, the system does not use cloud technology.

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.

PHILLIP CAUTHERS

Digitally signed by PHILLIP CAUTHERS
Date: 2024.02.06 09:50:24 -08'00'

Privacy Officer, Phillip Cauthers

MARLENE MOORE

Digitally signed by MARLENE MOORE
Date: 2024.02.06 07:47:51 -06'00'

Information Systems Security Officer, Marlene Moore

DENA LISTON

Digitally signed by DENA LISTON
Date: 2024.02.05 16:55:24 -05'00'

Information Systems Owner, Dena Liston

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).

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

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

SORN 121VA10 / 88 FR 22112 "National Patient Databases-VA"
https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

SORN 147VA10 / 86 FR 46090 "Enrollment and Eligibility Records-VA"
https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.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