Privacy Impact Assessment for the VA IT System called:

Pharmacy Reengineering Inbound ePrescribing Assessing Enterprise Program Management Office Veteran Health Administration Office

Date PIA submitted for review:

January 20, 2022

System Contacts:

<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Kamilah Jackson</td>
<td><a href="mailto:Kamilah.jackson@va.gov">Kamilah.jackson@va.gov</a></td>
<td>513-288-6988</td>
</tr>
<tr>
<td>Information System</td>
<td>Kristopher Parker</td>
<td><a href="mailto:Kristopher.Parker@va.gov">Kristopher.Parker@va.gov</a></td>
<td>405-456-4256</td>
</tr>
<tr>
<td>Security Officer (ISSO)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information System</td>
<td>Dena Liston</td>
<td><a href="mailto:Dena.Liston@va.gov">Dena.Liston@va.gov</a></td>
<td>304-886-7367</td>
</tr>
<tr>
<td>Owner</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Abstract

The abstract provides the simplest explanation for “what does the system do?” and will be published online to accompany the PIA link.

The Inbound ePrescribing (eRx) system receives inbound electronic prescriptions (e-prescriptions or eRxs) from an external provider (e.g., a doctor not associated with the Department of Veterans Affairs [VA], medical staff at a Department of Defense [DoD] military treatment facility, etc.) with the ability to process (fill, dispense, etc.) them in the Veterans Health Information Systems and Technology Architecture (VistA) Outpatient Pharmacy (OP) package. eRx also provides the capability to electronically transfer a prescription from a VA pharmacy to a different pharmacy, as well as electronically receive a transferred prescription from a different pharmacy.

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:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- Indicate the ownership or control of the IT system or project.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- A general description of the information in the IT system and the purpose for collecting this information.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether 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.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes.
- Whether the completion of this PIA could potentially result in technology changes
- 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 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.
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.

System users or typical clients are the users of the GUI/App itself and there are 1792 users registered in the GUI schema users table that access the GUI for Pharmacy Management, Tracking/Auditing and Reporting for Rx’s in the VA. Affected individuals would be any patient in the VA that will have script filled and sent to a VA Pharmacy.

The application itself is centrally deployed at Austin Information and 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.

To the best of our knowledge, there aren’t any changes to business processes as a result of the completion of this PIA.

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.

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:
PII Mapping of Components

Pharmacy Reengineering Inbound ePrescribing Assessing consists of 5 key components Pentaho, [WebLogic (eRx GUI application, eRx services application)], Oracle RDBMS, VistA, and Change Healthcare. 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.

### PII Mapped to Components

**Note:** Due to the PIA being a public facing document, please do not include the server names in the table.

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>VistA</td>
<td>Yes</td>
<td>Yes</td>
<td>Patient Internal Entry Number (IEN), Name, Date of Birth (DOB), Mailing Address, Zip</td>
<td>Authoritative system of record for</td>
<td>VA Policies governing VistA medical</td>
</tr>
</tbody>
</table>

<<Add Additional Information Collected But Not Listed Above Here (For Example, A Personal Phone Number That Is Used As A Business Number)>>
<table>
<thead>
<tr>
<th>Application</th>
<th>Access</th>
<th>Privileges</th>
<th>Data Used</th>
<th>Storage and Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>eRx GUI Application (WebLogic)</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>eRx Service Application (WebLogic)</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Oracle RDBMS</td>
<td>No</td>
<td>Yes</td>
<td>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).</td>
<td>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.</td>
</tr>
</tbody>
</table>
1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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.

1.4 How will the information be checked for accuracy? How often will it be checked?

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 system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract. This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

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.

1.5 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 Title 38, United States Code, Section 7301(a).


“79VA10 – Veterans Health Information Systems and Technology Architecture (VistA) Records-VA”
2020-28340.pdf (govinfo.gov)
Current SORN List (va.gov)

24VA10A7 Patient Medical Records – VA

142VA114 Community Residential Care and Medical Foster Home Programs-VA
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.

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. The risk is in revealing this information to an unauthorized party.

**Mitigation:** 2-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 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.
Name: Used to identify the patient (i.e., Veteran or employee)

Social Security Number: Used as official patient (i.e., Veteran or employee identifier)

Date of Birth: Used to identify the patient (i.e., Veteran or employee) and determine age of patient

Mailing Address: Used to communicate with patient (i.e., Veteran or employee)

Zip Code: Used to communicate with patient (i.e., Veteran or employee)

Phone Number(s): Used to communicate with patient (i.e., Veteran or employee)

Email Address: Used to communicate with patient (i.e., Veteran or employee)

Health Insurance Beneficiary Numbers Account numbers: used for patient (i.e., Veteran or employee) billing and cost recovery

Certificate/License numbers: used for external provider credentialing

Current Medications: Used for healthcare & prescribing medicine

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.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

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.

2.3 How is the information in the system secured?

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

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information 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.

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.

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:
- 2-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 GFE laptops, CAG, VA workstations. All three means of access are subject to standard VA encryption.
2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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.

Add answer here:

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.

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.

**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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

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.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

The prescription record retention may be governed by Pharmacy Service control schedule 7400.11 Prescription File. Per “New RCS- Final- 1.16.20.pdf,” the disposition instructions are “Temporary. Destroy after 3 years.” However, if a provider places a prescription into the Electronic health record, that information takes on the disposition date of the electronic health records of 75 years after last care received.

For the purpose of Inbound eRx, VistA is the system of record for this information, and disposition would be controlled by the associated records control schedule. 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).

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?

This question is related to privacy control DM-2, Data Retention and Disposal

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans’ Affairs VA Directive 6371, Destruction of Temporary Paper Records (April 2014), https://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=742&FType=2. 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 the VA Directive 6500, VA Cybersecurity Program, NIST SP 800-88 rev 1, Guidelines for Media Sanitization https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf and the VA Media Sanitization User’s Guide (November 17, 2014). 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 based on the VA Media Sanitization User’s Guide.

Additionally, Enterprise VistA and the facilities follow FSS Bulletin #209.1 National Media Sanitization and Destruction Program, as well as OIT-OIS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

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. Have policies and procedures been developed to minimize the use of PII 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.

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:** 2-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

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared /received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veterans Health Administration</td>
<td>VistA</td>
<td>System Log Files, sample clinical data that may contain Protected Health Information (PHI)</td>
<td>Electronically pulled from Vista through Computerized Patient Record System (CPRS)</td>
</tr>
<tr>
<td>Department of Veterans Affairs</td>
<td>VA Master Person Index (MPI)</td>
<td>Name, Social Security Number, Date of Birth, Sex/Gender, Mother’s</td>
<td>Site to site encrypted with TLS 1.2</td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared/received with the specified program office or IT system</td>
<td>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Veterans Health Administration</td>
<td>Maiden Name, Multiple Birth Indicator, Place of Birth (City and State), SSN Verification Status, Pseudo SSN</td>
<td>Veteran Patient Identification (VPID)</td>
<td>Web Service</td>
</tr>
</tbody>
</table>

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. 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

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared/received/transmitted with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is 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.

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/ViewPublication.asp?pub_ID=1090

24VA10A7 Patient Medical Records – VA
79VA10 – Veterans Health Information Systems and Technology Architecture (VistA) Records-VA”
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

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)

The VHA Notice of Privacy Practices provides information to a patient (i.e., Veteran) on their patient rights (i.e., to request a restriction).

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 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)

The VHA Notice of Privacy Practices provides information on the uses and disclosures of information that require their authorization.

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.

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:** VHA provides patients with copies of the Notice to Privacy Practices upon enrollment for care and every three years after, or when there are changes.

### 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?**

*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.*

*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).*

*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. This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.*

Prescription records processed by Inbound eRx become part of the patient’s health record within VistA. Patient requests for information are governed by VHA health information management and privacy policy with respect to right to access one’s own health record upon receipt of a written and signed request. All requests for copies of health records are processed by Release of Information staff at each VA medical center or accessed through the My HealtheVet premium account.

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.

Procedures for an individual submitting an amendment to their health records are addressing VHA Directive 1907.01 and 1605.01. Amendment requests are to be signed and submitted over the signature of the individual to whom the records pertain to the VA facility where they receive their health care.

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 VHA Notice of Privacy Practices provides information on the patients (e.g., Veteran) right to request and amendment of their health record.

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

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

The VHA Notice of Privacy Practices provides information on the patients (e.g., Veteran) right to request and amendment of their health record.

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.

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 individual may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt.

**Mitigation:**
VHA mitigates the risk of incorrect information in an individual’s records by authenticating the identity of the patient using the full name and date of birth (DOB). Additionally, staff verifies information in health records and corrects information identified as incorrect during each patient’s medical appointments.

VHA staffs Release of Information (ROI) offices at facilities to assist patients (i.e., Veterans) with obtaining access to their health records and other records containing PII and PHI.

The Veterans’ Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their health records. The Veteran must enroll in MHV with a premium account to obtain access to all the available features.

- In addition, VHA Directive 1907.01 Health Information Management and 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?**
Describe the process by which an individual receives access to the system.

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

2-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.

8.2 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 TMS system.

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

*If Yes, provide:*

1. The Security Plan Status,
2. The Security Plan Status Date,
3. The Authorization Status,
4. The Authorization Date,
5. The Authorization Termination Date,
6. The Risk Review Completion Date,
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

*Please note that all systems containing SPI are categorized at a minimum level of “moderate” under Federal Information Processing Standards Publication 199.*

*If No or In Process, provide your Initial Operating Capability (IOC) date.*

ATO Granted On: 02/16/2021

ATO Category: Full ATO

ATO Duration: 3 Years

FIPS 199 Classification: Moderate

**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).

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.

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)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

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

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

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

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

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

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

N/A
## Summary of Privacy Controls by Family

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

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

KAMILAH M. JACKSON 105810
Digitally signed by KAMILAH M. JACKSON 105810
Date: 2022.01.28 14:14:58 -05'00'

Privacy Officer, Kamilah Jackson

Kristopher A. Parker 1627705
Digitally signed by Kristopher A. Parker 1627705
Date: 2022.02.01 14:20:53 -06'00'

Information Systems Security Officer, Kristopher Parker

dena liston
Digitally signed by dena liston
Date: 2022.02.01 16:46:39 -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).

A copy of the VHA Notice of Privacy Practices is found here
https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090

24VA10A7 Patient Medical Records – VA
79VA10 – Veterans Health Information Systems and Technology Architecture (VistA) Records-VA”
Current SORN List (va.gov)