Privacy Impact Assessment for the VA IT System called:

VA Direct (DIR)

Veterans Health Administration

eHealth Exchange

Date PIA submitted for review:

6-8-2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Peggy Pugh	Margaret.Pugh@va.gov	202-731-6843
Information System Security Officer (ISSO)	Patricia Alleyne	Patricia.Alleyne@va.gov	512-529-8689
Information System Owner	Christopher Brown	Christopher.Brown1@va.gov	202-270-0599

Abstract

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

The VA Direct is developed as a user interface or medium through which VA users can utilize the Direct infrastructure to send, review and process Direct messages. The API (Admin Panel) serves as a system interface to the Direct infrastructure, from existing VA systems, to leverage Direct capabilities. Through use of the Direct Secure Messaging infrastructure, electronic health information can be shared with Federal Agency Partners and Non-VA care providers with trusted Direct compliant systems. Direct Secure Messaging is configured to use Personal Identity Verification (PIV) authentication using certificates only and hosted at Austin Information Technology Center (AITC).

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. The IT system name and the name of the program office that owns the IT system.

VA Direct (DIR), Veterans Health Administration

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

The VA Direct is developed as a user interface or medium through which VA users can utilize the Direct infrastructure to send, review and process Direct messages. The API (Admin Panel) serves as a system interface to the Direct infrastructure, from existing VA systems, to leverage Direct capabilities. Through use of the Direct Secure Messaging infrastructure, electronic health information can be shared with Federal Agency Partners and Non-VA care providers with trusted Direct compliant systems. Direct Secure Messaging is configured to use Personal Identity Verification (PIV) authentication using certificates only and hosted at AITC.

C. Indicate the ownership or control of the IT system or project.

VA Owned and VA Operated IS

2. Information Collection and Sharing

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

The source of DIR information is from Master Person Index (MPI), Cerner Joint Health Information Exchange (HIE), VA care providers and VA Staff. Their information is being stored to the local DIR mail database servers.

E. A general description of the information in the IT system and the purpose for collecting this information.

DIR information is being sent and received electronically as email messages. Information collected by the system is maintained by the Veterans and VA clinician staff. Data is saved and archived to the local DIR mail database servers.

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

DIR shares information with MPI and Cerner JHIE through https.

G. 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.

No. VA health partners and providers use DIR to manage VA health care information and documents online. DIR users obtain the credentials, authority, or role. Access to all messages will be made available to a search by authorized users even if they were not originally a member of the message recipient group or distribution list. DIR will include two (2) check boxes for secure electronic transmission of information to and from non-VA providers. Prior to sending a Direct message which contains 7332 protected conditions to non-VA providers, Direct users will be required to check the boxes regarding the presence or non-presence of 7332 protected conditions.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

24VA10A7 Patient Medical Records – VA - The DIR system's legal authority is the Title XIII of the American Recovery and Reinvestment Act (ARRA) of 2009. ARRA includes the Health Information Technology for Economic and Clinical Health (HITECH) Act, 'Title 38, United States Code, Sections 501(b) and 304."

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

No

D. System Changes

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

No

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

No

Section 1. Characterization of the Information

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

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

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

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

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

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*
- ☐ 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)

Other information maintained in the system: Biometrics

PII Mapping of Components (Servers/Database)

VA Direct consists of **3** key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **VA Direct** 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	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
Database Server	Yes	Yes	Patient data (First Name, Last Name, SSN, and DOB) in the form of attachments and CCDs, which contain phone, address, and relative data.	To securely send messages with attachments to internal and external partners regarding the care of Veterans/Patients and their dependents.	Encrypted messaging to internal and external partners who have registered as a Direct User.
Proxy/Mail Gateway Server	No	No	User information is passed to Web Server	User information is temporarily collected as it is passed to the Web Server.	Requires HTTPS connection using PIV (two factor authentication).
Application/Web Server	Yes	No	Patient data (First Name, Last Name, SSN, and DOB) in the form of attachments and CCDs, which contain phone, address,	The Webserver collects the information/data stored by the Database server	Encrypted messaging to internal and external partners who have registered as a Direct User.

			and relative data.		

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

The source of DIR information is from MPI, Cerner Joint HIE, VA care providers and VA Staff. Their information is being stored to the local DIR mail database servers.

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.

VA Direct uses MPI and Cerner Joint HIE, VA care providers, and VA staff because these are the data sources that will most benefit the VA Direct system. VA Direct does not use data from a commercial aggregator or from public Web sites.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

VA Direct does not create any score, analysis, or report for external use.

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?

DIR information is being sent and received electronically from MPI, Cerner Joint HIE, VA care providers and VA Staff electronically as encrypted email messages. Information collected by the system is maintained by the Veterans and VA clinician staff. Data is saved and archived to the local DIR mail database servers.

1.3b 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.

No, VA Direct does not collect information on a form and is not subject to the Paperwork Reduction Act. The Direct Trust Federated Services Agreement (FSA) covers HISP to HISP messaging.

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 DIR system provides the automated functionality to monitor the Consolidated Clinical Document Architecture (C-CDA) saving process and generate meaningful alerts for the DIR participants upon malfunctions or error conditions. Prior to sending the messages using DIR, the participants must review the notice and consent information and authorize to send the information. Information will be encrypted with digital signature.

1.4b 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.

VA Direct 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

The DIR system's legal authority is the Title XIII of the American Recovery and Reinvestment Act (ARRA) of 2009. ARRA includes the Health Information Technology for Economic and Clinical Health (HITECH) Act provisions that can be found at http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf. 24VA10A7 Patient Medical Records https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

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: Data maintained in the DIR database is classified as a mixture of Sensitive and Non-Sensitive, depending upon the source and nature of the data. DIR information is being sent and received electronically as email messages. Data elements include - First and Last Name, SSN, DOB, Phone, Address, Email, Medications, Medical Records, Financial, and Biometrics. Due to the sensitive nature of this data, there will be a risk that, if the data were accessed by an unauthorized individual or otherwise breached; serious personal, professional, or financial harm may result for the individuals affected.

Mitigation: VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow VA 6500 Handbook, and NIST SP800-53 high impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of this facility' common security controls. These issues are identified and described in the system security plans for the individual information systems. Prior to sending the messages using DIR, the participants must review the notice and consent information and authorize to send the information. Information will be encrypted with digital signature.

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: Veteran's identification
Social Security Number: used to verify Veteran identity and as a file number for Veteran
Date of Birth: used to verify Veteran identity
Mailing Address: Used to correspond with the Veteran
Zip Code: part of the mailing address
Phone Number(s): Used to correspond with the Veteran
Email Address: Used to correspond with the Veteran
Current Medications: Used to record current health and medical conditions of the veterans such as: health problems, diagnosis, therapeutic procedures, X-rays, laboratory tests, and operations.
Previous Medical Records: Used to record the history of health and medical conditions of the veterans such as: Health problems, diagnosis, therapeutic procedures, X-rays, laboratory tests, and operations.

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.

DIR does not analyze any patient data. The system is designed to provide security, privacy, data integrity, authentication of senders and receivers, and confirmation of delivery consistent with the data transport needs for health information exchange. The system is a secure email application that enables participants to send encrypted health information directly to known, trusted recipients over the internet.

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.

VA Direct 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?

DIR has encryption compliant and meets the VA6500 requirements for data at rest encryption as well as data in transit.

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

DIR has additional encryption protection; Information is only available to certain users (VA Database System Admins).

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

Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization using Network Identification (NTID) are all measures that are utilized within the facilities. The principle of need-to-know is strictly adhered to by the VA personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system.

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

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. ***<u>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.</u>***

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

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

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?

VA health partners and providers use DIR to manage VA health care information and documents online. DIR users obtain the credentials, authority, or role. Access to all messages will be made available to a search by authorized users even if they were not originally a member of the message recipient group or distribution list. DIR will include two (2) check boxes for secure electronic transmission of information to and from non-VA providers. Prior to sending a Direct message which contains 7332 protected conditions to non-VA providers, Direct users will be required to check the boxes regarding the presence or non-presence of 7332 protected conditions.

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

VA Records Management Policy (VA Handbook 6300.1) and the VA Rules of Behavior are in place to mitigate some of the risk that information is not handled properly. All VA annual privacy and security awareness training is recorded in the Talent Management System (TMS). The rules of behavior (VA handbook 6500 Appendix D) govern how veterans' information is used, stored, and protected.

2.4c Does access require manager approval?

VA Identity Access Management (IAM) / Master Person Index (MPI) Authentication does require manager approval. Data entry by VA staff integrity is enforced by instantiation of a multi-factor authentication requirement for logging onto the system.

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

VA Network Authentication is used to restrict access to appropriate personnel. Access is monitored, tracked, and logged.

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

All VA Direct staff are responsible for protecting PII and the use of proper procedures pertaining to safe handling and prevention of inappropriate distribution of 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*

The information listed in Section 1.1 is retained in the DIR database.
Name
Social Security Number
Date of Birth
Mailing Address
Zip Code
Phone Number(s)
Email Address
Emergency Contact Information (Name, Phone Number, etc. of a different individual)
Current Medications
Previous Medical Records
Other information maintained in the system: Continuity of Care Document (CCD), Job Title, Department, Organization, Location, and External Email.

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.*

NARA guidelines as stated in RCS 10-1 records retention schedule requires retention for 75 years. Whenever technically feasible, all records are retained indefinitely in the event of additional follow-up actions on behalf of the individual. However, any documents that the veteran requests removal from the system will be purged from the system upon request.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes, all records stored within the system of record indicated on an approved disposition authority, The records retention schedule is named for its predecessor system, Administrative Data Repository VA. Further details on the Administrative Data Repository are located at: https://www.govinfo.gov/content/pkg/FR-2008-11-26/pdf/E8-28183.pdf

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

NARA guidelines as stated in RCS 10-1 records retention schedule requires retention for 75 years. Additionally, Item number 7900 – The Caregiver Record Management Application (CARMA) record description states the disposition authority as DAA-0015-2020-0001-0001. Whenever technically feasible, all records are retained indefinitely in the event of additional follow-up actions on behalf of the individual. However, any documents that the Veteran requests removal from the system will be purged from the system upon request.

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.

Under the jurisdiction of Veteran Health Administration (VHA), it is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws, the General Records Schedule (GRS) and VHA Records Control Schedule (RCS) 10-1. The GRS can be found at www.archives.gov.VA Directive 6300, Records and Information Management contains the policies and responsibilities for VA's Records and Information Management program. VA Handbook 6300.1, "Records Management Procedures", Section 3.2, contains mandatory procedures for the proper management of eliminating data at the end of the retention period. Procedures are enforced by Records Management Staff and VA Records Officers.

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.

Test Patients with mock names, social security numbers and medical records are used for testing, demonstration, and training purposes. Direct Secure Messaging product development teams do not use or store real patient data in Direct's lower-level environments.

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 risk to maintaining data within the DIR system is the longer time frame information is kept, the greater the risk that information possibly will be compromised, unintentionally released, or breached.

Mitigation: To mitigate the risk posed by information retention, DIR adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, DIR will carefully dispose of the data by the determined method as described in question 3.4.

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***
My Health eVET (MHV)	Database Server	•Name •SSN •Phone Number •Address •Email •Health/Medical Information (Diagnosis, Treatment, Medication and X-Ray) •Financial Information •Biometrics	Pull data HTTPS/443 thru AITC Network Proxy to DIR Database via SQL Server/1433
Other VA Clinical Systems	Database Server	•Name •SSN •Phone Number •Address •Email	Pull data HTTPS/443 thru AITC Network Proxy to DIR Database via SQL Server/1433

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*
		•Health/Medical Information (Diagnosis, Treatment, Medication and X-Ray) •Financial Information •Biometrics	
VA User Workstation	Application/Web Server	•Name •SSN •Phone Number •Address •Email •Health/Medical Information (Diagnosis, Treatment, Medication and X-Ray) •Financial Information •Biometrics	Pull data HTTPS/443 thru AITC Network Proxy to DIR Application Mail Server via SMTP/(25, 465,587)
API Admin Panel (Web Browser)	Application/Web Server	•Name •SSN •Phone Number •Address •Email •Health/Medical Information (Diagnosis, Treatment, Medication and X-Ray) •Financial Information •Biometrics	Pull data HTTPS/443 thru AITC Network Proxy to DIR Application/Web Server via HTTP/80

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: There is a risk that information may be shared with an unauthorized VA program, system, or individual. The privacy risk associated with maintaining PII is that sharing data within

the Department of Veteran's Affairs could happen and that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization using Network Identification (NTID) are all measures that are utilized within the facilities. The principle of need-to-know is strictly adhered to by VA personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is 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***
My Health eVet (MHV)	To provide summary of care document for treatment purposes.	• Name • SSN • Phone Number • Address • Email • Health/Medical Information (Diagnosis, Treatment, Medication and X-Ray) • Financial Information • Biometrics	24VA10A7 Patient Medical Records and Administrative Data Repository - VA	Pull data HTTS/443 thru AITC Network Proxy to DIR Database via SQL Server/1433
Other VA Clinical Systems	To provide summary of care document for treatment purposes.	• Name • SSN • Phone Number • Address • Email • Health/Medical Information (Diagnosis, Treatment, Medication and X-Ray) • Financial Information • Biometrics	24VA10A7 Patient Medical Records and Administrative Data Repository - VA	Pull data HTTS/443 thru AITC Network Proxy to DIR Database via SQL Server/1433
VA User Workstation	To provide summary of care document for treatment purposes.	• Name • SSN • Phone Number • Address • Email • Health/Medical Information (Diagnosis, Treatment, Medication and X-Ray) • Financial Information • Biometrics	24VA10A7 Patient Medical Records and Administrative Data Repository - VA	Pull data HTTS/443 thru AITC Network Proxy to DIR Database via SQL Server/1433
API Admin Panel (Web Browser)	To provide summary of care document	• Name • SSN • Phone Number • Address	24VA10A7 Patient Medical Records and	Pull data HTTS/443 thru AITC Network

	for treatment purposes.	• Email • Health/Medical Information (Diagnosis, Treatment, Medication and X-Ray) • Financial Information • Biometrics	Administrative Data Repository - VA	Proxy to DIR Database via SQL Server/1433

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: There is a risk that information may be shared with an unauthorized VA program, system, or individual and expose the personal and health information of the patients. This information, if exposed could lead to identity theft.

Mitigation: Safeguards implemented to ensure data is not sent to outside of the VA organizations intended are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized to prevent exposure outside of the VA.

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.

Additional notice is provided by the system's System of Record Notice (SORN), 24VA10A7 Patient Medical Records and 150VA19 Administrative Data Repository -VA, which can be viewed at the following link: https://www.govinfo.gov/content/pkg/FR-2008-11-26/pdf/E8-28183.pdf A third form of notice is provided by this Privacy Impact Assessment, which is available online as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii).

The VHA Notice of Privacy Practices provides information to a patient (i.e., Veteran) on VHA's authority to collect their private health information.

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

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

The VHA Notice of Privacy Practices provides information to a patient (i.e., Veteran) on VHA's authority to collect their private health information.

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

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 collect their private health information.

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

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.

VHA Directive 1605.01, Privacy and Release Information, Paragraph 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. 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.

The VHA Notice of Privacy Practices provides information to a patient (i.e., Veteran) on their right to consent to uses of their information.

The Notice states "To request a restriction, you must submit a written request that identifies the information you want restricted, when you want it to be restricted, and the extent of the restrictions. All requests to restrict use or disclosure should be submitted to the facility Privacy Officer at the VHA health care facility that provided or paid for your care."

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

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

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

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

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

Privacy Risk: Only assigned role users for the system are allowed access to participant's data in the system. There is a risk that VA employees, employee veterans and other members of the public will not know that the DIR exists or that it collects, maintains, and/or disseminates PII and other SPI about them.

Mitigation: If an assigned user no longer requires access to the system, the user account can be de-activated by the program administrator.

Section 7. Access, Redress, and Correction

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

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

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

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

VHA Directive 1605.01 'Privacy and Release Information', Paragraph 7(b) states the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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).

VA Direct 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.

VA Direct is not exempt from the access provisions of the Privacy Act.

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.

Under the jurisdiction of VHA, VHA Directive 1605.01 'Privacy and Release Information', Paragraph 8 states the rights of the Veterans to amend to their records via submitting VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

In case the information in the DIR system is inaccurate, the veterans have the right to request amendment of erroneous information in accordance with the Privacy Act and HIPAA Privacy Rule. Individuals 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 the Veteran's information. In response, you may do any of the following: • File a "Statement of Disagreement".• Ask that your initial request for amendment accompany all future disclosures of the disputed health information.• https://www.justice.gov/opcl/privacy-act-1974

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.

If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before, and state that the documentation they are now providing supersedes those previously provided.

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 the individual accidentally provides incorrect information when entering the information.

Mitigation: Veterans send and receive encrypted email messages. Any validation performed would merely be the veteran personally reviewing the information before they send or accept it. Individuals are allowed to provide updated information for their records by updating the information and indicating that the new information supersedes the previous data.

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.

Office of Information and Technology (OIT) documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. This documentation and monitoring is performed through the use of Talent Management System (TMS). Access to the system is granted to VA employees and contractors by the local authority within each administrative area staff office, following the described account creation process.

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 outside of the VA that will have access to VA Direct.

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.

There's no different path beside following the Office of Information and Technology (OIT) documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. This documentation and monitoring is performed through the use of Talent Management System (TMS). Access to the system is granted to VA employees and contractors by the local authority within each administrative area staff office, following the described account creation process.

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.

Contracts of DIR are authorized VA and contract employees are reviewed annually by the OIT contracting offices. There are contract system administration personnel within the Austin Information Technology Center (AITC) who maintain the server hardware and software but are not privileged users of the DIR system itself.VA contract employee access is verified through VA personnel before access is granted to any contractor. Contracts and contractor access are reviewed annually at a

minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training (TMS#10176) documented in TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Contractors with access to PHI are required to complete HIPAA (TMS# 10203) privacy training annually. Contractors have current BAA in effect when accessing PHI/PII.

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

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

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB (for AITC technicians) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the DIR user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. DIR users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* June 9, 2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* May 5, 2023
5. *The Authorization Termination Date:* August 4, 2023
6. *The Risk Review Completion Date:* Sept 28, 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.***

N/A

Section 9 – Technology Usage

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

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

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

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

No

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

N/A

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

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

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

N/A

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

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

N/A

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

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

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

Margaret L. Pugh 104985

Digitally signed by Margaret L. Pugh 104985
Date: 2023.06.14 07:13:37 -04'00'

Privacy Officer, Peggy Pugh

PATRICIA ALLEYNE

Digitally signed by PATRICIA ALLEYNE
Date: 2023.06.13 15:30:37 -05'00'

Information Systems Security Officer, Patricia Alleyne

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2023.07.05 15:44:58 -05'00'

Information Systems Owner, Christopher Brown

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
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

50VA19 Administrative Data Repository – VA
http://www.gpo.gov/fdsys/pkg/FR-2008-11-26/pdf/E8-28183.pdf

HELPFUL LINKS:

Record Control Schedules:

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

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

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