Privacy Impact Assessment for the VA IT System called:

Vaultara Flight-I (Vaultara-i)

Veterans Health Administration (VHA)

VISN 20 Northwest Health Network

Date PIA submitted for review:

November 4, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Todd Miles	Todd.Miles@va.gov	360-619-5902
Information System Security Officer (ISSO)	Vincent Panettiere	Vincent.Panettiere@va.gov	718-836-6600 x7727
Information System Owner	Fred Tolley	Fred.Tolley@va.gov	202-461-9005

Abstract

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

Vaultara Flight platform is hybrid-SaaS solution that consists of an on-prem "console" that communicates with Vaultara FLARE services hosted in AWS GovCloud. The Flight solution enables efficient exchange of Clinical/Medical Images & Information (i.e. studies, reports) electronically, securely, and cost-effectively between VA facilities and approved Veteran's Choice Act (Mission Act) providers and other outsourced exam resources.

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.*
Name: Vaultara Flight-I (Vaultara-i); System Owner of on-prem console: VHA Medical Device Protection Program; Business Owner of SaaS/Cloud FLARE platform: VISN 20 Healthcare Technology Management

B. *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
The Flight solution enables efficient exchange of Clinical/Medical Images & Information (i.e. studies, reports) electronically, securely, and cost-effectively with approved Veteran's Choice Act (Mission Act) providers and other outsourced exam resources.

C. *Indicate the ownership or control of the IT system or project.*
Business Owner: VISN 20 Healthcare Technology Management

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.*
Any veteran in the encatchment area of VISN 20 being referred to the community for care and needing to share records with the VA from their community care visit(s). This system will also allow VISN 20 VA facilities to exchange records from veteran visits at other VA facilities outside of VISN 20.

E. *A general description of the information in the IT system and the purpose for collecting this information.*
Images and PDF files containing medical images and study results from patient visits.

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

See technical description from vendor below.

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.*

System will be utilized at eight VISN20 facilities. See technical description below for how system is used and how PII is maintained at each site.

3. Legal Authority and SORN

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

PO

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?*

N/A- It is not in the process of being modified. CSP does not have access to the SORN, so cannot validate the coverage.

D. System Changes

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

N/A-No.

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

N/A-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)

The Medical Record field is retained within the records, but has already been altered at the Console to swap the Social Security Number for the Accession Number

PII Mapping of Components (Servers/Database)

Vaultara Flight has been analyzed to determine if any components of the system collect PII. The type of PII collected by Vaultara Flight 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
On-prem Vaultara virtual server at each VISN 20 facility	Yes	Yes	Patient Name Patient DOB Patient SSN/MRN/Accession Number Patient Sex Patient Race/Ethnicity Patient treatment Records/Documentation Physician Name	Provide access to digital copies of exams and clinical documentation	During transmission, the information is double encrypted using 2048-bit encryption methods. During storage, the information Version Date: February 27, 2020 Page 8 of 33 is encrypted using FIPS 140-2 approved algorithms. Patient SSN is modified from original information to Accession

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?

Transactions from a VA's Console into the Flare environment obtain their data from VA's internal database/storage systems, typically known as PACS (Picture Archiving and Communication Systems) that obtain images from medical devices such as CTs, MRIs, X-rays, etc.

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.

PACS systems are a centralized repository of medical images.

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

Vaultara-i

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?

Information collected by a VA's Console is obtained from VA's internal database/storage systems, typically known as PACS (Picture Archiving and Communication Systems) that obtain images from medical devices such as CTs, MRIs, X-rays, etc

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*.*

N/A.

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.

Vaultara ensures that the data received corresponds to the VA user's transaction and requested information. There are also native corruption safeguards in place inherent to TCP/IP which DICOM communications use which prevents VA from opening data if data was corrupted. Additionally, there are data integrity checks that Vaultara performs on data upload and downloads that verifies whether the data received is whole and without corruption.

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 can also perform audit checks on received studies to ensure that the patient data (Name, DOB, MRN, Sex, etc) matches requested data.

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

Privacy Act of 1974 Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. Freedom of Information Act (FOIA) 5 USC 552 VA Directive 6500 Managing Information Security Risk: VA Information Security Program. The legal authorities that defined the collection of information include: U.S. Code Title 38 Veterans' Benefits, Part V, Chapter 73, Subchapter 11, Section 7330C. "Quadrennial Veterans Health Administration Review" (b)(C)(3). Systems of Records Notices applicable to this system are: 150VA19, "Administrative Data Repository-VA", November 26, 2008; 138VA005Q, "Veterans Affairs/Department of Defense Identity Repository (VADIR)-VA", July 27, 2009

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk:
Disclosure of personally identifiable information, that if disclosed may expose the respondent/subject to financial loss or identity theft. Disclosure of medical, personal, or other information that may compromise the individual's reputation, circumstances, or safety. Disclosure of participation in a study or activity, where knowledge of participation may adversely impact the individual's reputation or circumstances.

Mitigation:
Information will be secured on the system through access controls, personnel security awareness and training, regular auditing of information and information management processes, careful monitoring of a properly authorized information system, control of changes to the system, appropriate handling and testing of contingencies and contingency planning, ensuring that all users of the information system are properly identified and authorized for access, and that they are aware of the rules and acknowledge that fact, by ensuring that any incident is handled expeditiously, properly maintaining the system and regulating the environment the system operates in, controlling media, evaluating risks and planning for information management and information system operations, by ensuring that the system and any exchange of information is protected, by maintaining the integrity of the system and the information stored in it, and by adhering to the requirements established in applicable contracts. Data integrity checks help ensure data does not become corrupted and all data is encrypted in transit and at rest.
Additionally, the following security controls lower the risk of unwarranted disclosure of PHI.

VA implements the following security measures and controls on Vaultara:

- Identification and Authentication - User Access control is managed by strong authentication method and must be assigned on the "Least Privilege" Principal. VA utilizes "two-factor authentication" for general users. A separate token and non-mail enabled account is required for users who require elevated privileges on IT systems.

- Logical Access Controls - VA accounts are separated into domains and the system administrators only manage those accounts within their domain. Accounts are audited every ninety (90) days. VA policy requires account termination within twenty-four (24) hours of an employee/contractor departure. Accounts are terminated immediately in the event of a hostile termination.
- Physical and Environmental Security - Physical and environmental controls are maintained at VA facilities. Badges are required for employees and contract staff. Access to networking closets and computer rooms require authorization from the facility Chief Information Officer (CIO) and a log is maintained. VA computer rooms are environmentally controlled for operation of the equipment is contains. This includes power; network; heating, ventilation, and air conditioning (HVAC); and fire suppression.
- Firewall, IDS, and Encryption - Intrusion detection systems (IDS) are in place at gateways and throughout the VA network. The VA's Network Security Operations Center monitors the VA network 24x7. Suspicious activity is reviewed and determined recommendations are formulated and assigned to the system administrators. FIPS 140-2 validated encryption is required for transmission of sensitive information.

Vaultara implements the following security measures and controls:

- Identification and Authentication - Vaultara uses access control systems to identify individual users and prevent unauthorized users from accessing information systems owned or maintained by Vaultara. The authentication and identification policy dictates constraints for Vaultara employee logins and passwords and puts access controls into place. The access controls are subject to review: the CSO reviews all information system users and to ensure proper roles have been assigned within the information resource environment. Version Date: February 27, 2020 Page 12 of 33
- Logical Access Controls - Vaultara implements all security controls as described in the ATO System Security Plan ("SSP"). These security controls include, but are not limited to the following Flight Flare Services account policies:
    * access to Flight Flare Services is limited to authorized users only
    * a unique account for accessing Flight Flare Services is automatically created by transactions initiated by a VA users on the Flight Console
    * VA users must provide recipient's email address to which access emails are sent o recipients are assigned a one-time password upon account creation o passwords must be comprised of
        - a minimum of 8 characters
        - one upper case, one lower case, one special character and one number
        - must have a minimum of 4 characters changed from the prior password
    * passwords need to be:
        - changed every 90 days
        - unique (up to 24 prior passwords or within 2 years, whichever is the longer)
    * passwords can't be changed within 24 hours of a prior password change
    * accounts are locked out for 30 minutes if an incorrect password is entered more than twice
    * users are bound by inactivity policies (5 mins) after which they are prompted (for a maximum of 30 seconds) to keep their session alive, otherwise are automatically logged out

* secured via multi-factor authentication ("MFA") using mobile device and timed one-time password ("TOTP") authentication o disabled if dormant for ninety (90) days o re-enabled by VA Console Administrators or Vaultara support personnel only

- Physical and Environmental Security - The AWS environment is subject to AWS security policies which includes (but not restricted to) least privilege and time-based access, user access reviews, logging, 24/7/365 Closed Circuit Television (CCTV) monitoring and professional security staff.
- Firewall, IDS, and Encryption - Vaultara' s encryption policies outline all methods required for both internal use and for all Vaultara Flight services products and services. The policy explains both transfer security and validation of encrypted data and traffic for all Vaultara Flight products. The policy additionally outlines the maintained AWS infrastructure security requirements.

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.

The data exchanged between VA facilities, veterans, and third-party healthcare providers would facilitate completion of VA/VHA Medical Record of Approved Outsourced Care and help VA fulfill the Veteran Choice Act (i.e. MISSION ACT). Transitioning to Vaultara Flight architecture would: 1) provide a reliable method to exchange patient records with outside providers. (2) reduce personnel time and costs associated to acquiring and packaging exams physical transport. (3) reduce the need or avoid conducting repeat exams due to platform importing compatibility related issues. (4) simple user-interface via Vaultara to easily pull up and route exam results to/from external customers. (5) This communication conduit is not limited to only Radiology, DICOM, etc. This solution would benefit all 'Ologies', ROI (Release of Information), and medical center services. Simply put, this is the essence of medical image/ information sharing. When complete patient information, interoperative reports, and associated images are readily available across the continuum of care, quality care is provided. Data Elements used are those listed below that are present as part of the medical study that is exchanged: Patient Name Patient DOB Patient SSN/MRN/Accession Number Patient Sex Patient Race/Ethnicity Patient treatment Records/Documentation Physician Name

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.*

Vaultara does not currently provide data analysis capabilities. However, VA can analyze the data obtained through Vaultara on other internal/VA systems. The data obtained/exchanged through Vaultara is described in sections above.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

The data obtained/exchanged through Vaultara is described in the section above.

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?
Secure TLS over TCP/IP 443 using encryption 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?

All data is encrypted in transit and at rest. SSN’s are replaced automatically with an Accession Number.

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

A list of the additional security controls Vaultara has in place to safeguard PII/PHI is available in section 1.7.

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. ***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:

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

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

User authenticates with the system and is granted specific permissions according to their role. Access to PII is determined through user input which searches source database systems.

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

User manuals are provided which document procedures required.

2.4c Does access require manager approval?

Access is granted through membership of Active Directory groups within the organization. Access to those groups requires managerial approval.

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

Yes.

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

Both the VA and Vaultara have responsibility in assuring safeguards for PII within the system. Details regarding responsibility can be found in section 1.6.

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, Date of BirthSex, Health Insurance Beneficiary Numbers, Previous Medical Records, Race/Ethnicity, Medical Record Number, Medical images, Medical studies/reports/results from patient visits

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

The information is retained according to the retention policy assigned to each individual transaction, dictated by the date assigned by the authorized user of Console of said transaction. When submitting a transaction, the Console is configured to work with three dates when referring to the retention policy: the minimum date (by default set to 2 days from the current date), the default date (by default, set to 5 days from the current date) and the maximum date (by default, set to 12 days from the current date). All three dates are used when the user selects the calendar control within the Console interface. A console user, with administrative privileges, can configure these defaults, which would apply to all users of that Console.

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?

Vaultara complies with retention policies approved by the National Archives and Records Administration (NARA).

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

The maximum allowable retention period is 90 days for any records within Vaultara. The guidance for retention of records is found in the RCS 10-1, and the National Archives and Records Administration. The RCS 10-1 can be found at: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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

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

Once the retention policy set by the VA user has expired for a given transaction, and assuming that no other transactions relate to the specific records in question, the system deletes the records from the encrypted file system by use of an automatic maintenance script. This maintenance script is run daily between the hours of midnight and 2am UTC.

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.

An authorized user for a Send Image transaction has the option to select "anonymize" (de-identify) as for all selected records within that transaction. When selected, this option overwrites all PII related meta-data fields with either default, or null values, as set by an authorized user with administrative permissions. This happens automatically during the processing of a Send Image transaction. With all other transactions, the system is unable to automatically de-identify the data being sent and therefore becomes the sole responsibility of the authorized user submitting the transaction: said user must check a confirmation tool before any transaction is submitted to Console, which specifically states they are responsible for ensuring that all relevant PII information is removed.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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:

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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:

<u>Privacy Risk:</u> Vaultara allows VA administrator-defined retention policies to minimize the risk assumed by data retention.

<u>Mitigation:</u> Vaultara allows VA administrator-defined retention policies to minimize the length of time data is retained per transaction/exchange over Vaultara. When the retention data is reached for a record, Vaultara disposes of the data by the methods described in question 3.4. Said retention policies are followed in accordance with the VA Records Control Schedule RCS 10-1. The Privacy Officer, Information Security Officer, and Chief Information Officer also monitor controls to mitigate any breaches of security and privacy.

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***
VA Medical PACS servers at VISN 20 facilities (Radiology and/or other PACS databases (i.e. Dental, Cardiology PACS)	To efficiently exchange Clinical/Medical Imaging & Information electronically, securely, and costeffectively with approved Veteran's Choice Act (Mission Act) providers, veterans, and other VA facilities.	Patient Name Patient DOB Patient SSN/MRN/Accession Number Patient Sex Patient Race/Ethnicity Patient treatment Records/Documentation Physician Name	TCP/IP and DICOM

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 PII could be shared with an inappropriate VA organization or institution.

Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, Version Date: February 27, 2020 Page 20 of 33 identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, program management, planning and maintenance. There is required HIPAA training for users of the system, and PII/PHI is on a need-to-know basis. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation.

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***
Vaultara Flight FLARE Services (hosted on AWS GovCloud and functions as intermediary platform for exchanging data with patients, third party healthcare providers, and other VA facilities)	To complete patient medical records by exchanging with approved Veteran's Choice Act (Mission Act) providers, veterans, and other VA facilities.	Patient Name Patient DOB Patient SSN/MRN/Accession Number Patient Sex Patient Race/Ethnicity Patient treatment Records/Documentation Physician Name	VA-Vaultara National MOU/ISA and VA VISN 20-Vaultara BAA	Secure TLS over TCP/IP 443 using encryption in transit and at rest

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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 PII could be shared with an inappropriate organization or institution.

Mitigation: Security controls described in sections 1.7 and 2.3 apply and minimize risk of PII availability to unauthorized organizations. The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, Version Date: February 27, 2020 Page 22 of 33 system information integrity, security assessment and authorization, incident response, risk assessment, program management, planning and maintenance. There is required HIPAA training for users of the system, and PII/PHI is on a need-to-know basis. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation.

Section 6. Notice

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

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

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

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

The two SORNs that allow Vaultara to collect personal information are 150VA19 and138VA005Q.

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

N/A.

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 legal authority to use and collect SSNs to support digital identities is provided through Title 44 United States Code Section 3551-3558, Federal Information Security Modernization Act (FISMA) of 2014 and Title 5 United States Code Section 522(a).

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.

When a patient is the end user, he/she chooses to provide information to the VA through Vaultara for care that the patient opted into through MISSION ACT/VA CHOICE Program. When VA-contracted third-party healthcare providers are the end user of Vaultara, the care and records they provide for said care are approved by the patient through release of information documentation governed by each healthcare provider. A patient who receives care through a MISSION/CHOICE provider has opted into receiving care and consented to providing information; this is accomplished through VA purchased care processes. If a patient does not want to receive care and/or provide information through VA CHOICE Program, they may choose to opt out or not to participate.

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.

Yes, the patient has the opportunity to consent or deny uses of information during opt-in processes for the VA CHOICE Program. He/She also has the opportunity to consent or deny uses of information when presented with release of information documentation from VA-contracted healthcare providers.

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:

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: An individual is unaware that their information is being collected by the system.

Mitigation: When a patient is the end user of the system, he/she controls input of his/her information and therefore is aware what information is and is not provided. When a VA-contracted healthcare provider is the end user of the system, the patient is made aware of information sharing at various times during the application process for participating in the program. No federal agencies or other organizations have access to the PII data and, per the Privacy Policy, this information is not shared without the individual's permission.

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.***

A patient can request to obtain any information that was exchanged using Vaultara through standard VA processes governing release of patient information. VA staff can utilize logs available in Vaultara to provide data that was exchanged using Vaultara. Data that is obtained using Vaultara and is ingested by internal VA systems gets marked, and VA staff can provide information on any data exchanged using Vaultara upon request.

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).

N/A.

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.

N/A.

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.

Data exchanged through Vaultara is reviewed prior and upon receipt and is always exchanged through Patient Name, DOB, Sex, MRN, and ordered study matching. Once data is ingested into an internal VA system from an exchange through Vaultara, data can be corrected using the internal VA system if needed.

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.

Verification and correction of any erroneous data exchanged through Vaultara is standard operating procedure without notification to the patient.

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.

Redress is available upon request and permitted through standard release, complaint, and correction of information processes within the VA.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

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:
<u>Principle of Individual Participation:</u> Is the individual provided with the ability to find out whether a project maintains a record relating to him?

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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:

<u>Privacy Risk:</u> There is a risk of incomplete records on information exchanged through Vaultara. There is also a risk that individuals whose records contain incorrect information may not receive notification on how to redress or correct their information.

<u>Mitigation:</u> An individual can request access and correction to any of their information. Vaultara keeps a log studies sent by the VA. VA also marks permanently stored data that is ingested into internal VA systems. VA Office of Purchased Care also maintains records on outsourced care/exams for each patient. Third party providers also possess studies/data on exams they provide to patients.

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.

Vaultara uses access control systems to identify individual users and prevent unauthorized users from accessing information systems owned or maintained by Vaultara.
All access to Vaultara Flare is controlled by:

- a unique account for accessing Flight Flare Services is automatically created by transactions initiated by a VA users on the Flight Console
- VA users must provide recipient's email address to which access emails are sent
- recipients are assigned a one-time password upon account creation
- passwords must be comprised of
  ▪ a minimum of 8 characters
  ▪ one upper case, one lower case, one special character and one number
  ▪ must have a minimum of 4 characters changed from the prior password
- passwords need to be
  ▪ changed every 90 days
  ▪ unique (up to 24 prior passwords or within 2 years, whichever is the longer)
- passwords can't be changed within 24 hours of a prior password change
- accounts are locked out for 30 minutes if an incorrect password is entered more than twice
- users are bound by inactivity policies (5 mins) after which they are prompted (for a maximum of 30 seconds) to keep their session alive, otherwise are automatically logged out
- secured via multi-factor authentication ("MFA") using mobile device and timed one-time password ("TOTP") authentication
- disabled if dormant for ninety (90) days
- re-enabled by VA Console Administrators or Vaultara support personnel only

All access to Vaultara Console is controlled by:

- Identification and Authentication - User Access control is managed by strong authentication method and must be assigned on the "Least Privilege" Principal. VA utilizes "two-factor authentication" for general users. A separate token and non-mail enabled account is required for users who require elevated privileges on IT systems.
- Logical Access Controls - VA accounts are separated into domains and the system administrators only manage those accounts within their domain. Accounts are audited every ninety (90) days. VA policy requires account termination within twenty-four (24) hours of an employee/contractor departure. Accounts are terminated immediately in the event of a hostile termination.
- Physical and Environmental Security - Physical and environmental controls are maintained at VA facilities. Badges are required for employees and contract staff. Access to networking closets and computer rooms require authorization from the facility Chief Information Officer (CIO) and a log is maintained. VA computer rooms are environmentally controlled for operation of the equipment is contains. This includes power; network; heating, ventilation, and air conditioning (HVAC); and fire suppression.
- Firewall, IDS, and Encryption - Intrusion detection systems (IDS) are in place at gateways and throughout the VA network. The VA's Network Security Operations Center monitors the VA network 24x7. Suspicious activity is reviewed and determined recommendations are formulated and assigned to the system

administrators. FIPS 140-2 validated encryption is required for transmission of sensitive information.

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?

Access to PII is granted by authorized users of the system and such users are required to confirm a use of conduct banner before submission. Users from other agencies have read-only roles to the specific PII granted to them.

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Roles are determined by membership of Active Directory groups. Specific groups provide access to respective sources of information. Administrative roles are provided through membership of administrative Active Directory group and configured as such on the system.

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.

Non-application users are limited to Vaultara support personnel. Vaultara's access and use of data is governed by a BAA and an MOU/ISA established between VA and Vaultara.

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

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

All VA users and Vaultara support personnel are required to complete annual Privacy Security Training, as well as VA Rules of Behavior training and mandated privacy HIPAA training.

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:* December 18 2020
3. *The Authorization Status:* Authorization to Operate
4. *The Authorization Date:* June 3, 2021
5. *The Authorization Termination Date:* June 2, 2024
6. *The Risk Review Completion Date:* June 1, 2021
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Section 9 – Technology Usage

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

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

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

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

The system uses AWS GovCloud technology and is currently awaiting review for its FedRAMP ATO.

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.*

The BAA and MOU/ISA ID: E-2120 between the contractor and VA address this. The current year contract # is 36C26022P0991 and also stipulates that the following security provisions are adhered to:

- *44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"*
- *FIPS Pub 201, "Personal Identity Verification of Federal Employees and Contractors," March 2006*
- *5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"*
- *42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"*
- *VA Directive 0710, "Personnel Suitability and Security Program," September 10, 2004*
- *VA Directive 6102, "Internet/Intranet Services," July 15, 2008*
- *36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003*
- *Office of Management & Budget (OMB) Circular A-130, "Management of Federal Information Resources," November 28, 2000*
- *32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"*
- *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008*
- *Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998*
- *Homeland Security Presidential Directive (12) (HSPD-12)*
- *VA Directive 6500, "Information Security Program," August 4, 2006*
- *VA Handbook 6500.6, "Contract Security," March 12, 2010*
- *Program Management Accountability System (PMAS) portal (reference PWS References – Technical Library at https://www.voa.va.gov/)*

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.

Vaultara collects and owns ancillary data.

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.

Yes. Please refer to the BAA, MOU/ISA ID: E-2120, and contract #36C26022P0991 established between VA and vendor.

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).

RPA systems are in place, in order to process transactions that contain PII/PHI information. The autonomy of removing elements of PII/PHI is performed without human interaction for security purposes.

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

ID	Privacy Controls
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

TODD A. MILES 677038 Digitally signed by TODD A. MILES 677038
Date: 2023.09.27 14:48:32 -07'00'

Privacy Officer, Todd Miles

Vincent J. Panettiere 1368456 Digitally signed by Vincent J. Panettiere 1368456
Date: 2023.09.28 11:13:32 -04'00'

Information System Security Officer, Vincent Panettiere

FRED TOLLEY Digitally signed by FRED TOLLEY
Date: 2023.09.28 08:47:54 -04'00'

Information System Owner, Fred Tolley

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).

150VA19 Administrative Data Repository-VA

https://www.govinfo.gov/content/pkg/FR-2008-11-26/pdf/E8-28183.pdf

138VA005Q Veterans Affairs/Department of Defense Identity Repository (VADIR)-VA

https://www.govinfo.gov/content/pkg/FR-2022-12-23/pdf/2022-27988.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