Privacy Impact Assessment for the VA IT System called:

Vaultara Flight

Office Of Veterans Health Administration (VHA) OIT (Office Of Info and Technology)

Date PIA submitted for review:

December 18, 2020

System Contacts:

<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Todd Miles</td>
<td><a href="mailto:Todd.Miles@va.gov">Todd.Miles@va.gov</a></td>
<td>(360)-619-5902</td>
</tr>
<tr>
<td>Information System</td>
<td>Andrew Vilailack</td>
<td><a href="mailto:Andrew.Vilailack@va.gov">Andrew.Vilailack@va.gov</a></td>
<td>(813) 970-7568</td>
</tr>
<tr>
<td>Security Officer (ISSO)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information System</td>
<td>Terrill Harrison</td>
<td><a href="mailto:Terrill.harrison@va.gov">Terrill.harrison@va.gov</a></td>
<td>(202)-461-5408</td>
</tr>
<tr>
<td>Owner</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Abstract

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

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:

- **The IT system name and the name of the program office that owns the IT system.**
  - Name: Vaultara Flight
  - System Owner of on-prem console: VHA Medical Device Protection Program
  - Business Owner of SaaS/Cloud FLARE platform: VISN 20 Healthcare Technology Management

- **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.

- **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.

- **If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?** An on-prem console will be installed at eight VISN 20 facilities on an MDIA VLAN.

- **A general description of the information in the IT system.** Images and PDF files containing medical images and study results from patient visits.

- **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.

- **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.

- **A citation of the legal authority to operate the IT system.** PO
• Whether the completion of this PIA will result in circumstances that require changes to business processes N/A- No.
• Whether the completion of this PIA could potentially result in technology changes N/A- No.
• If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? N/A- No, this is a new system and is not in the process of being modified. /ISSO
• Does the system use cloud technology? 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. Yes, it utilizes cloud technology and is undergoing VA FedRAMP sponsorship and authorization at a moderate impact level. /PM
• Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? Yes. VA owns the data through the approved outsourcing agreements managed through VA purchased care processes. Per contract and MOU/ISA between the VA and Vaultara, Vaultara provides the platform to exchange said data and protect it in compliance with all VA standards.
• 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? Yes, it is described and stipulated in the purchase agreement between VA and Vaultara as well as in the MOU/ISA between VA and Vaultara.
• What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected? Information that contains PII, should it become compromised, could potentially have serious impact on the reputation of the Veterans Affairs. This would not cause significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions could be significantly reduced. This could potentially result in significant damage to organizational assets or result in significant financial loss. The compromise of data could potentially also result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries. If an individual’s privacy related data is disclosed, it could result in a fraudulent act or identity theft by a criminal or an unauthorized individual. /PO

The Vaultara “Flight” solution consists of a virtual machine residing on a local area network (one per VHA site) configured to work with a SaaS residing in a FedRAMP approved environment. The local virtual machine is known as the Vaultara Management Console (“Console”) and is only ever accessed by authorized VA users local to its installed location; the SaaS environment is known as Vaultara’s “Flare”, and is available to anyone with an internet connection.

Transactions
Transactions are processed through the Flight solution enabling data to be sent between a VA site and a designated 3rd party. Transactions are referred to by their functionality and are named in relation to the Console from which they originated from: transactions that send data from the VHA to a 3rd party are known as “send” transactions; those that will permit a 3rd party to send information into the VHA are known as a “receive” transactions.
All transactions originate and are initiated from a Console: data is selected by an authorized user and based upon their choice of transaction.

**Payloads**
For any type of transaction, the collection of binary files that are being transmitted between the Console and Flare systems is known as the “payload”.

**Send transactions**
Every send transaction is associated to a specific patient and the user enters general query information, typically based upon a patient’s name or unique medical record identifier (“Patient ID”) into the Console. The Console uses that query information to obtain a list of qualifying patients from existing systems on the VHA network (typically a PACS configured to work with the Console). The user selects which patient the transaction is to be related to and then proceeds to complete the transaction. Send transactions are categorized as one of two types: “Send Images” and “Send Files”.

**Send Files transactions**
For a Send Files transaction, the user chooses how long the 3\textsuperscript{rd} party can access the transaction for (known as the “retention period”) and then sets the payload for the transaction by selecting files (either individually or by folder) from an accessible resource: typically, a folder residing on a network share or locally to the workstation being used. Those files are uploaded immediately to the Console and then processed (see “Processing send transactions”).

**Send Image transactions**
For a Send Image transaction, a list of studies relating to the queried patient is presented to the user. The user selects from this list which study/studies are to be shared with, how long the transaction is available, and what permissions are available to, the 3\textsuperscript{rd} party. Optionally, study related information documentation (in the form of PDF files) may be added to the transaction by the user; as can a complete patient de-identification of the study be performed. The transaction is then submitted to the Console. The Console contacts the identified PACS and requests copies of the selected study/studies using industry standard DICOM protocols. Once the Console has confirmed that it has successfully received said study/studies it preps those files (and any related PDF documents) for the transaction to proceed.

In every case of a Send Image transaction undertaken by a VHA Console (and irrespective of the de-identification option chosen by the user for that transaction) the Patient ID meta-data field content of each DICOM image is replaced with the data residing in the Accession Number field of that same image: this is to ensure that the Patient ID of the patient is not available to the 3\textsuperscript{rd} party, as that field (for VHA sites) contains the Social Security Number (“SSN”) of the patient in question.

**Processing receive transactions**
There is no payload for setting up a receive transaction. Through a TLS1.2 secure connection, Console notifies Flare that a receive transaction has been permitted for a specific 3\textsuperscript{rd} party.

**Processing send transactions**
Once the payload is ready for transmission, the Console encrypts the payload using FIPS 140-2 certified encryption libraries and a per transaction password. The transaction password is encrypted to Flare’s public RSA key via an asymmetric pre-assigned public key infrastructure system. All encryption algorithms are compliant with FIPS 140-2, using AES 256bit keys in CBC mode. The entire payload is split up into easily transferrable slices (“chunks”) and each chunk transferred over TLS1.2 connections to the Flare environment.
The Flare environment employs an EFS mounted file system which has been configured to only permit encrypted internal file-streams and automatically encrypts all data at rest. Additionally, Flare uses a clustered database system that only permits encrypted connections from internal systems and utilizes encryption at rest for its internal data storage.

Flare receives each transmitted chunk in memory, writing that chunk to the EFS when complete. Upon receiving all chunks for a specific transaction, the chunks are validated using SHA1 hashing techniques and are re-assembled if none are deemed to be corrupt. The password for the transaction is decrypted using the private RSA key and the now decrypted payload placed into a separate EFS folder.

If a Send Image transaction permits the 3rd party to view those images online, the DICOM images are extracted and sent to Flare’s DICOM server which is configured to only accept TLS1.2 connections, populates its database using Flare’s database cluster and stores its copy of the DICOM images on the EFS. Database tables are populated permitting only the respective 3rd party user access to the study/studies that relate to those DICOM images.

Send File (and Send Image, if permitted) transaction payloads are compressed into a zip file and placed in a per transaction folder, residing on the EFS. Database tables are populated permitting only the respective 3rd party user access to refer to the zip file.

Once all processing is complete, the initial (decrypted) payload files are automatically removed from their location on the EFS.

Whilst the payload has been processing, Flare also ascertains if the 3rd party has ever used the system before. If this is the first time, the system automatically sets up an account and assigns a one-time password to that 3rd party’s account. The contents of two emails are generated (known as the “Welcome 1” and “Welcome 2” emails) and when the transaction processing is complete, a third email is generated (known as a notification email).

**Emails**

The content of 3rd party emails is generated but not sent by Flare. Such emails are associated to a specific transaction and therefore a specific Console. Via TLS 1.2 connections to Flare, the Console requests the content of any emails that need to be sent to a 3rd party and in turn, sends those emails out through the locally configured mail server on the VHA network. Emails never contain direct links to any transactions, rather inform the 3rd party of their account set up (full login credentials never sent in the same email, as outlined by HIPAA guidelines) and notifications of subsequent transactions that are pertinent to that specific 3rd party.

**3rd Party Login**

When notified by email, a 3rd party is prompted to log into Flare in order to review their transaction. All connections to Flare happen over a TLS1.2 connection. The 3rd party is prompted to enter their credentials and (should it be their initial login) immediately prompted to change the password (that was automatically generated by the system, as noted above) and complete an MFA security process in which a mobile phone is used to configure additional security checks during subsequent logins.

Once successfully logged in, 3rd parties are presented with various options, depending on permissions assigned to them from one or more transactions.
If permitted to view online studies, the user will be presented with a “View” link which, once selected, presents individual studies (that the 3rd party has been granted access to) listed in a table. Upon selecting of these studies, a subsequent authentication request asking for the patient’s date of birth is presented to the user. The user must enter the correct date before opening up the study in the online viewer.

If permitted to download a payload, the user will be presented with a “Download” link which, once selected, presents individual transactions listed in a table. Upon selecting of these studies, a subsequent authentication request asking for the patient’s date of birth is presented to the user. The user must enter the correct date before automatically downloading the transaction payload.

It’s worth noting that the date of birth authentication request occurs on the initial request for a specific transaction within the same web session. If a transaction has both view and download capabilities and the 3rd party has already authenticated against the transaction when (for example) viewing the study and remain in the same session, they will not be prompted again when selecting to download the zip file. Logging out of Flare, or closing their browser tab or browser completely, will invalidate the 3rd party’s session.

**Transaction Retention**
The length of time that a specific transaction is made available to a 3rd party is dependent on the retention period set by the user who initiated the transaction on Console. Retention periods are designated by a date and access to a transaction includes the entire 24-hour period up to and during that date. All retention dates are recorded in UTC.

If a 3rd party logs into Flare and the retention period for one or more of their transactions have expired, those transactions will no longer be listed in the user table and therefore inaccessible to access. Physical files relating to study/studies will remain within Flare until all related transactions’ retention periods have expired, after which Flare automatically removes the files.

If a 3rd party logs into Flare and chooses to remove a transaction from their available list, they may do so by selecting the “Delete” (trash) icon. Although this removes the transaction from the list, it does not affect the retention period of that transaction and therefore, Flare will still keep physical files related to that transaction until the retention period expires. This enables the user (through a support call) to request a previously removed transaction to be re-listed: the retention period remains the same date as the original, initiating transaction.

**Receive transactions (Flare)**
If a 3rd party logs into Flare and has a receive transaction assigned to them, they will be presented with an “Upload” permission. This entitles the 3rd party to upload files (or the content of a folder) from any accessible location available to their workstation to Flare. The 3rd party may perform multiple sessions for a single transaction, up to the retention period of said transaction after which their upload permissions are revoked.

An upload session consists of the 3rd party completing the form (briefly outlining details of the upload) and uploading their files to Flare.

Flare automatically scans the files for vulnerabilities, malware and viruses and if no issues arose from the scan, commences to encrypt the payload using FIPS 140-2 certified encryption libraries and a per transaction password. The transaction password is encrypted to Console’s public RSA key via an asymmetric pre-assigned public key infrastructure system. All encryption algorithms are compliant with
FIPS 140-2, using AES 256bit keys in CBC mode. The entire payload is split up into easily transferrable slices (“chunks”) waiting for Console to check in and download them for further processing.

**Receive transactions (Console)**

Console periodically calls Flare to ascertain if there are any 3rd party upload sessions that require processing and are associated to previously submitted receive transactions. If so, Console pulls down (over a secure TLS1.2 connection) each of the chunks from Flare associated to that receive transaction, writing that chunk locally to its file system. Upon receiving all chunks for a specific transaction, the chunks are validated using SHA1 hashing techniques and are re-assembled if none are deemed to be corrupt. The password for the transaction is decrypted using Console’s private RSA key and the now decrypted payload placed into a separate folder on the filesystem.

The decrypted payload is analyzed for any DICOM images and, if found, study related information is populated into the Console database; otherwise, the payload is compressed into a user accessible zip file. Console then notifies a pre-configured email address regarding the receive session, prompting an authorized Console user to review the received files. If DICOM images were received, the user has the option of altering basic meta-data fields relating to the DICOM images and can choose to have those manipulated images pushed to a PACS (or other DICOM node). Alternatively, the DICOM images may be pushed without changes to a PACS (or other DICOM node). Non-DICOM files are available to be downloaded as a zip file, extracted and used as seen fit by the user.

**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://www.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.
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 Account Information
- Health Insurance Beneficiary Numbers
- Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Other Unique Identifying Number (list below)

Add Additional Information Collected But Not Listed Above Here (For Example, A Personal Phone Number That Is Used As A Business Number)

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**

Vaultara Flight consists of two key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Vaultara Flight and the reasons for the collection of the PII are in the table below.

**PII Mapped to Components**

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-prem Vaultara virtual at each VISN 20 facility</td>
<td>Yes</td>
<td>Yes</td>
<td>Patient Name Patient DOB Patient SSN Patient Sex Study Description</td>
<td>Provide access to digital copies of exams and clinical documentation</td>
<td>During transmission, the information is double encrypted using 2048-bit encryption methods. During storage, the information</td>
</tr>
</tbody>
</table>
1.2 What are the sources of the information in the system?

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

Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

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

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

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.

1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2.

Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?

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

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

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.
1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose. This question is related to privacy control AP-2, Purpose Specification.

The data being collected from third party healthcare providers, other VAs, and/or veterans helps ensure that the VA has complete medical records on a given patient.

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

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

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

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.

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

1.6 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, 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.


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;

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

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

**Principle of Data Quality and Integrity:** Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

**Privacy Risk:**
 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.
• 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:
  o access to Flight Flare Services is limited to authorized users only
  o a unique account for accessing Flight Flare Services is automatically created by transactions initiated by a VA users on the Flight Console
  o 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
  o passwords need to be
    ▪ changed every 90 days
    ▪ unique (up to 24 prior passwords or within 2 years, whichever is the longer)
  o passwords can’t be changed within 24 hours of a prior password change
  o accounts are locked out for 30 minutes if an incorrect password is entered more than twice
  o 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
  o 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.

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

Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

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

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

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.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project
covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

**Principle of Transparency:** Is the PIA and SORN, if applicable, clear about the uses of the information?

**Principle of Use Limitation:** Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Access to PII in Vaultara is governed by the security controls below.

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.
• 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:
  o logical access to the console are dictated by VA policies above, i.e. users must be members of VA governed AD groups, and passwords are governed by VA GPOs
  o access to Flight Flare Services is limited to authorized users only
  o a unique account for accessing Flight Flare Services is automatically created by transactions initiated by a VA users on the Flight Console
  o 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
  o passwords need to be
    ▪ changed every 90 days
    ▪ unique (up to 24 prior passwords or within 2 years, whichever is the longer)
  o passwords can’t be changed within 24 hours of a prior password change
  o accounts are locked out for 30 minutes if an incorrect password is entered more than twice
  o 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
  o 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 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 Birth
Sex
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. 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)? If so please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. This question is related to privacy control DM-2, Data Retention and Disposal.
Vaultara complies with retention policies approved by the National Archives and Records Administration (NARA), with a maximum allowable retention period of 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 of SPI?

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

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

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?*

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

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 PRIVACY IMPACT ASSESSMENT: Retention of information

*Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.*

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains.
information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

**Principle of Minimization:** Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

**Principle of Data Quality and Integrity:** Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged? This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

**Privacy Risk:** Vaultara allows VA administrator-defined retention policies to minimize the risk assumed by data retention.

**Mitigation:**
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. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

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

*State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.*
For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

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

Data Shared with Internal Organizations

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA Medical PACS servers at VISN 20 facilities (Radiology and/or other PACS databases (i.e. Dental, Cardiology PACS)</td>
<td>To efficiently exchange Clinical/Medical Imaging &amp; Information electronically, securely, and cost-effectively with approved Veteran’s Choice Act (Mission Act) providers, veterans, and other VA facilities.</td>
<td>Pt Name, DOB, SSN that is converted to accession number, Sex</td>
<td>TCP/IP and DICOM</td>
</tr>
</tbody>
</table>

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. This question is related to privacy control UL-1, Internal Use.

Follow the format below:

**Privacy Risk:** 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,
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: This question is #7 in the Privacy Threshold Analysis.

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

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties.
Data Shared with External Organizations

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>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)</td>
<td>To complete patient medical records by exchanging with approved Veteran’s Choice Act (Mission Act) providers, veterans, and other VA facilities.</td>
<td>Pt Name, DOB, MRN, Sex</td>
<td>VA-Vaultara National MOU/ISA and VA VISN 20-Vaultara BAA</td>
<td>Secure TLS over TCP/IP 443 using encryption in transit and at rest</td>
</tr>
</tbody>
</table>

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

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

Follow the format below:

**Privacy Risk:**
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,
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 notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

The two SORNs that allow Vaultara to collect personal information are 150VA19 and 138VA005Q. 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 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

**Principle of Transparency:** Has sufficient notice been provided to the individual?

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

Follow the format below:

**Privacy Risk:**
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?**

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

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

*If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information. This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.*

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.

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

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

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

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department’s access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program’s effectiveness because the individuals involved might change their behavior.

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

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

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

Follow the format below:

Privacy Risk:
There is a risk 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.

Mitigation:
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?

Describe the process by which an individual receives access to the system.

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

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

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.
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 it 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.
8.2 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 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?

If Yes, provide:

1. The date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and
4. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

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

If No or In Process, provide your Initial Operating Capability (IOC) date.
### Section 9. References

**Summary of Privacy Controls by Family**

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

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

TODD A. MILES 677038
Digitally signed by TODD A. MILES
677038
Date: 2021.02.01 13:28:37 -08'00'

Privacy Officer
Signature of Information Security Systems Officers

The Information Security Systems Officers below attest that the information provided in this Privacy Impact Assessment is true and accurate.

[Signature]

Digitally signed by ANDREW
VILA/LACK 1811006
Date: 2021.02.02 07:41:08 -05'00'
Signature of Area Manager

The Area Manager below attests that the information provided in this Privacy Impact Assessment is true and accurate.

Terrill N. Harrison
1079525

Digitally signed by Terrill N. Harrison
1079525
Date: 2021.03.03 12:57:54 -05'00'

Area Manager
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).