Privacy Impact Assessment for the VA IT System called:

Community Image Exchange Services (CIES)

Veterans Health Administration (VHA)

Health, Clinical Services, Diagnostics Sub-Product Line

eMASS ID # 2296

Date PIA submitted for review:

11/8/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kamilah Jackson	Kamilah.jackson@va.gov	513-288-6988
Information System Security Officer (ISSO)	Richard Alomar-Loubriel	Richard.alomar-loubriel@va.gov	787-641-7582
Information System Owner	John Di Lorenzo	John.DiLorenzo@VA.gov	520-529-1729

Abstract

The abstract provides the simplest explanation for "what does the system do?".

The Community Image Exchange System (CIES) is intended to exchange diagnostic images and related diagnostic reports between VA and Community Care Providers. The system follows security controls applicable for sensitive information systems with PII and PHI exchanges. The system relies heavily on Health Level 7 protocol (HL7 V2) and Digital Imaging and Communications in Medicine (DICOM) services and messages. The system is a connection between VHA imaging systems and external (Internet) connections for COTS vendor products, such as Vaultara, PowerShare, vCARE, and others to allow Community Care Providers to complete images for veterans who are receiving care from them. Example includes a veteran who lives remote from a VHA facility may need a Magnetic Resonance Imaging (MRI), Computerized Tomography (CT) scan, etc. and VHA Community Care determines that a local provider will be sent a consult. The Community Care Provider (CCP) schedules the patient for test. Once test is read by the local radiologist the DICOM image and associate report are sent to VHA via the CIES application. All data is DICOM images and associated reports in HL7 back to VHA. All communications go through VA Enterprise Cloud (VAEC) GovCloud on Port 443 through VA Gateways to vendor gateways which receive data from their CCP's who own licenses to their individual products. Within VHA the images will then be stored in the local VistA Imaging, Picture Archive and Communications System (PACS), and reports will be stored in VistA, VistA Imaging and other locations based on the local VHA facility systems configurations. Data elements include Patient Identifier (both internal VHA and external healthcare organization, Date of Birth, SSN (used within VHA imaging workflows as identifiers), and Consult Number sent from VHA to external organization.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

Community Image Exchange Service (CIES), Health, Clinical Services, Diagnostics Sub-Product Line

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

The Community Image Exchange System is intended to exchange diagnostic images and related diagnostic reports between VA and Community Care Providers. The system follows security controls applicable for sensitive information systems with PII and PHI exchanges. The system relies heavily on HL7 V2 and DICOM services and messages.

C. *Who is the owner or control of the IT system or project?*

Health, Clinical Services, Diagnostics Sub-Product Line

2. Information Collection and Sharing

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

CIES is a new system in development; however, the goal is an Enterprise implementation with potential access to all VA patients DICOM images with VistA, VistA Imaging, Picture Archive and Communications Systems (PACS). Over 5 million potentials in future years.

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

Goal is the ability to implement sharing of radiology and other images (x-ray, MRI, CT, etc.) between VA and Community Care Providers. Includes the ability to assign a Consult to external imaging organization when a VA patient is being seen by Community Care Providers.

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

DICOM images stored in VistA Imaging, PACS, and other internal VA systems, as well as reports stored in VistA related to those images may be shared. In addition, DICOM images and associated reports from Community Care Providers will be "pulled" from external sources into VA networks for storage at local VA medical centers.

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

Internal data sharing will include transmission via DICOM and HL7 standards. External transmission will be encrypted over Port 443. Initially CIES will operate at a limited number of sites, however overall goal is to be an Enterprise solution for image sharing. Each site will store images within their local VistA Imaging and/or PACS system. HL7 reports will be stored in VistA at each site.

3. Legal Authority and SORN

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

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

24VA10A7 Patient Medical Records-VA
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

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

No change will be necessary.

4. System Changes

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

New Platform as a Service (PaaS) being implemented for Enterprise sharing of images, some business processes will be changed.

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

No anticipated technology changes, CIES is implemented on Virtual Machine (VM) servers within the VAEC Amazon GovCloud environment.

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☐ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers

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

☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☒ Medical Record Number
☐ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements: Community Care Referral Number, Community Care Provider Medical Record Number

PII Mapping of Components (Servers/Database)

Community Image Exchange Services (CIES) consists of 2 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Community Image Exchange Services (CIES) and the reasons for the collection of the PII are in the table below.
Note: Due to the PIA being a public facing document, please do not include server names in the table.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Vaultara Gateway Server (VM)	***Yes, transmit***	***No***	***Medical Record Number, DOB, potentially SSN***	***Vendor connection to external portal where images are stored from CCP providers. Gateway server only transmits data and data is not stored within their Gateway Server.***	***FedRAMP, RMF***
PowerShare Gateway Server (VM)	***Yes, transmit***	***No***	***Medical Record Number, DOB, potentially SSN***	***Vendor connection to external portal where images are stored from CCP providers. Gateway server only transmits data and data is***	***FedRAMP, RMF***

				not stored within their Gateway Server.	
vCARE Gateway Server (VM)	***Yes, transmit***	***No***	***Medical Record Number, DOB, potentially SSN***	***Vendor connection to external portal where images are stored from CCP providers. Gateway server only transmits data and data is not stored within their Gateway Server.***	***FedRAMP, RMF***
Central Compass Router	***Yes, transmit***	***Yes***	***Medical Record Number, DOB, potentially SSN***	***Central Compass Router is a transmission mechanism that directs incoming information to the Compass Router at the VA Medical Center from which the CCP request was made. Data may be stored on the Central Compass Router for short periods while determining VAMC..***	***FedRAMP, RMF***

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?
Data comes from a variety of sources. Within the VA data comes from VistA and VistA Imaging and all users are authorized VA staff or contractors. Examples include a patient who has been approved for Community Care may have a consult to see a local imaging service to obtain a radiology study. That consult is sent from local VistA to the Community Care Provider. Returning data comes from these external providers through CIES and based on

information on the study the DICOM images and associated HL7 report are sent to the local facility and stored in VistA Imaging, Picture Archive and Communications System (PACS), or in some cases other VAMC systems. CIES will also communicate with Electronic Precision Scanning and Indexing (EPSI) for incoming HL7 reports and other documents which might require transformation and adding to the patient record.

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.
Data will not come from data aggregators.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?
Community Care Providers will use various vendor COTS packages to transmit images and reports to the vendor portal, which as mentioned in 1.2b above, which is then transmitted to the vendor gateway within CIES Accreditation Boundary.

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?
CIES collects but does not retain data. Data is collected from service-level requests from VistA, VistA Imaging, or Community Care systems and applications. A system user of VistA or Community Care may enter a request for a DICOM image where services are being provided by an external Community Care Provider (CCP) outside the VA healthcare system. These are often referred to as Consults or Referrals. The request transmits from VistA or Community Care application through CIES to the external CCP organization. Upon completion of the services the CCP provider will transmit the associate DICOM images and HL7 Report in various formats back through CIES where it is sent to various VA systems including VistA, VistA Imaging, Community Care and EPSI. The data is only maintained within CIES until it has been reviewed by appropriate HIMS, Radiology (or other services depending on the image type).

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?
Not applicable for CIES. CIES only transfers DICOM images and HL7 reports between VAMC sites and Community Care Provider (CCP) sites providing services on behalf of the VA. No documents are stored, only transmitted.

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.
When the file is received from community it goes to the local facility into a workflow for VI and radiology will look to make sure the image matches prior to the data being fully ingested into VistA using DICOM reconciliation workflow.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?
While CIES does not use commercial aggregators, the Office of Community Care coordinates care by Community Care Providers (CCP) for Veteran patients eligible for care under the Mission Act of 2018. These CCP organizations have their own Electronic Health Record (EHR), PACS, and other systems and applications. When a consult is being arranged with the CCP organization a requirement is established that data transmitted back to VA must include the VA patient identifier and Consult number to ensure accuracy. These requirements are outside the control of CIES VetsEZ Support Team or OIT. Upon return of DICOM images and HL7 reports each VAMC has staff who validate the incoming record prior to storing in VistA, VistA Imaging, PACS, etc. Community Care within VA then manages status reporting, billing and other relevant services associated with the Consult.

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

As documented earlier, CIES VetsEZ Support Team has developed the Community Image Exchange (CIES) Privacy SOP sets the following requirements: Title 38 Code of Federal Regulations (CFR) provides the legal authority that permits the collection of personally identifiable information (PII). VA Directive 6502 provides the legal authority that permits use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need. Before collecting PII, the VAEC AWS Privacy Officer (PO), Information System Security Officer (ISSO), and / or Information System Owner (ISO) determine whether the contemplated collection, use, maintenance, and sharing of PII is legally authorized for use in a specific program or information system. The authority to collect, use, maintain, and share PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation

such as Privacy Act Statements. VAEC AWS hosted in Amazon Web Services GovCloud Cloud locations. CIES transmits and temporarily stores some PII and PHI. CIES falls under the SORN for 79VA10 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: ***The system collects, processes, and retains PII and PHI on Veterans and on Members of the Public, primarily Community Care Providers. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal and financial harm to the individuals impacted and adverse negative effect to the VA.***

Mitigation: ***Data collected, processed, and retained will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.***

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system that will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.
CIES will use, at a minimum, the following information: 1) Social Security Number: Used as a patient identifier, currently the standard identifier for all VA imaging systems; 2) Date of Birth: Used as a secondary data field to confirm patient identity; 3) VA Patient Identifier: Used to ensure appropriate record is identified by facility prior to sending Consult; and 4) CCP Patient Identifier: Used by external organization, provided to VA in the event additional information is needed from CCP. This CCP Patient Identifier is created from the external healthcare organization and ensure we have the correct patient on their side which matches our VA Patient Identifier which is part of the CCP request or consult.

PII/PHI Data Element	Internal Use	External Use
Medical Record Number	File identification purposes	For ensuring record matches when returned from Community Care Provider
Community Care Referral Number	File identification purposes	Created by the Community Care Office application for identifying returned DICOM images matching patient requests
CCP Medical Record Number	For ensuring record matches when returned from Community Care Provider. This is the external healthcare organization patient identifier	File Identification purposes
SSN	File identification purposes	For ensuring record matches when returned from Community Care Provider
DOB	File identification purposes	For ensuring record matches when returned from Community Care Provider

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?
Data coming in from the vendor (Vaultara, PowerShare, vCARE) Gateway is received at the Central Compass Router where a Rabbit MQ message is created and sent to EPSI. Validation of required data fields is completed in both systems. Analysis is based on the Patient Identifier,

Consult Number, and in some cases the SSN. Some messages will include both the VA Patient Identifier and the Community Care Provider Patient ID number.

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.

All data received from Community Care Providers will be entered into the existing patient record in VistA, as well as DICOM images will be placed into VistA Imaging, PACS, and other storage mediums and again associated with the current patient record.
As documented earlier, CIES VetsEZ Support Team has developed the Community Image Exchange (CIES) Privacy SOP sets the following requirements: 1) CIES VetsEZ Support Team establishes and maintains database inventories, used by all programs and information systems, that contain, access, shares, or utilizes PII/PHI. 1) New CIES databases follow current requirements with placement on the encrypted VA Network. 3) CIES System owner/designee will pull a report containing PBC 65 type information for their system by following the instructions in the "ITOPS Database Operations Team Enterprise SQL Server Inventory Instructions" document. 4)The System Owner along with the Privacy Officer will review the database inventories and update them annually or as needed when significant changes occur. 5) CIES Information System Owner (ISO), Information System Security Officer (ISSO), and Privacy Officer (PO) will document the database inventories in the PTA and use this information to support the establishment of information security requirements for all new or modified information systems containing PII. 6) The PTA contains a listing of all information systems identified as collecting, using, maintaining, or sharing PII. 7) The PTA is reviewed, updated, and signed off on annually or as needed when significant changes occur.

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?
As documented earlier, CIES VetsEZ Support Team has developed the Community Image Exchange (CIES) System and Communications Protection (SC) SOP sets the following requirements: 1) The Information System Owner and/or Designee is responsible for validating that within high-impact systems, the information system protects the confidentiality and/or integrity of information at rest.
2)VAEC AWS defines and documents the information at rest that is to be protected.
3) Controls implemented to protect data at rest are documented in the System Security Plan (SSP).
4) VA has processes to protect information at rest or in storage that include but are not limited to:
4a - VA approved encryption such as FIPS 140-2 or current version
4aa - Full disk encryption (FDE)
4ab - Virtual disk and volume encryption and

4ac - File/folder encryption
5) Intrusion Detection and Protection Systems (IDPS) Firewall's rulesets
6) Endpoint security to scan for malware other threats to confidentiality and integrity.
7) Physical and logical access control mechanisms
8) Change control processes.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
VA within VistA Imaging is still using SSN as the primary identifier with VA imaging workflows; therefore, the patient's SSN will be listed as the primary patient identifier in every single DICOM image shared with community providers. All messages and transactions going outside VA are transmitted encrypted over Port 443 or Port 343.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
VA within VistA Imaging is still using SSN as the primary identifier with VA imaging workflows; therefore, the patient's SSN will be listed as the primary patient identifier in every single DICOM image shared with community providers. All internal VA data sources use encryption of data at rest and data in transit. All messages and transactions going outside VA are transmitted encrypted over Port 443 or Port 343 depending on if External or Internal to VA Networks.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?
Accounting of Disclosures for CIES is managed by VistA, patients may follow standard medical center procedures for requesting a copy of the records of access to their PII.
As documented earlier, CIES VetsEZ Support Team has developed the Community Image Exchange (CIES) Privacy SOP sets the following requirements:
1) VA Privacy Service in conjunction with the Senior Agency Official for Privacy (SAOP), the Privacy Compliance Assurance Office, and the Office of Enterprise Risk Management (ERM) are responsible for monitoring and auditing privacy controls continuously.

2) CIES VetsEZ Support Team and OIT monitors privacy controls, per organization-defined frequency, to ensure effective implementation.
Community Image Exchange (CIES) Privacy SOP sets the following requirements:

> ***VA Privacy Service develops a training and awareness strategy/program for VA Privacy Officers (POs) to ensure they understand the operations, privacy laws, regulations, practices, and standards that prescribe the activities and responsibilities of VA POs. The strategy/program outlines the path for the growth and development of POs serving in varied capacities.***
> ***Community Image Exchange (CIES) Privacy SOP sets the following requirements:***
> ***1) CIES VetsEZ Support Team privacy incident response plan (PIRP) provides an organized and effective response to privacy incidents and is included in the facility incident response plan (IRP).***
> ***2)When a privacy incident occurs the privacy officer (PO) will take the following actions:***
> ***2a - Utilize the Privacy Security Event Tracking System (PSETS) to enter a PSETS ticket to identify the complaint or incident.***
> ***2b -Report the privacy incident within one hour of notification to the Cyber Security Operations Center (CSOC) and Unites States Computer Emergency Readiness Team (US-CERT),***
> ***2c - Contact and inform individuals affected by the incident,***
> ***2d - Update the PSET ticket as the incident is investigated,***
> ***2e - And request CSOC to close the PESET ticket once the investigation has been completed, documented, and letters of the incident are mailed to the affected individuals.***
> ***System Administrators and Developers may access PII during system checks, while checking issues with operational functionality, or while reviewing logs. All CIES VetsEZ Support Team members have completed appropriate HIPAA and Privacy training requirements.***

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

As documented earlier, CIES VetsEZ Support Team has developed the Community Image Exchange (CIES) Privacy SOP sets the following requirements:
2) CIES VetsEZ Support Team and OIT monitors privacy controls, per organization-defined frequency, to ensure effective implementation.
Community Image Exchange (CIES) Privacy SOP sets the following requirements:
1) VA Privacy Service develops a training and awareness strategy/program for VA Privacy Officers (POs) to ensure they understand the operations, privacy laws, regulations, practices, and standards that prescribe the activities and responsibilities of VA POs. The strategy/program outlines the path for the growth and development of POs serving in varied capacities.
Community Image Exchange (CIES) Privacy SOP sets the following requirements:
1) CIES VetsEZ Support Team privacy incident response plan (PIRP) provides an organized and effective response to privacy incidents and is included in the facility incident response plan (IRP).
2) When a privacy incident occurs the privacy officer (PO) will take the following actions:

2a - Utilize the Privacy Security Event Tracking System (PSETS) to enter a PSETS ticket to identify the complaint or incident.
2b -Report the privacy incident within one hour of notification to the Cyber Security Operations Center (CSOC) and Unites States Computer Emergency Readiness Team (US-CERT),
2c - Contact and inform individuals affected by the incident,
2d - Update the PSET ticket as the incident is investigated,
2e - And request CSOC to close the PESET ticket once the investigation has been completed, documented, and letters of the incident are mailed to the affected individuals.

2.4c Does access require manager approval?

Yes, the appropriate VA Manager approves all system access to CIES. This follows standard VA Elevated System Privilege access processes.

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

As described in the CIES PTA, CIES is not access by users. Only System Administrators and Developers have direct access to the system and data. This does potentially include access to PII. All access is monitored via Audit Logging. All other access for user access to data is via either local VAMC VistA, VistA Imaging, PACS and potentially local medical devices downstream from these systems.

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

The Information System Owner is responsible for assuring safeguards of all PII. Data is safeguarded by 1) data encryption for data at rest, 2) data encryption for data in transit, and 3) use of Port 443 for all data transmitted external to VA networks.

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
As documented earlier, CIES VetsEZ Support Team has developed the Community Image Exchange (CIES) Privacy SOP sets the following requirements: 1) CIES VetsEZ Support Team is responsible for limiting collection of PII relevant and necessary to accomplish the legally authorized purpose of collection described in the System of Records Notice (SORN), Privacy Act Statement, and for which the individual has provided consent. 2) CIES VetsEZ Support Team follows VA Directive 6309 (2)(a) to:
• Ensure that the collection of information is needed.
• Is not unnecessarily duplicative.
• Reduces, to the extent feasible, the burden on respondents.

• Is written in clear and understandable terms.
• And is to be implemented in a way consistent with existing reporting and record keeping practices and that the records are retained for the length of time outlined within the record keeping requirement (General Records Schedule or Records Control Schedule.
3) CIES VetsEZ Support Team is responsible for conducting an initial evaluation of personally identifiable information (PII) holdings, via the PTA, and submitting the PTA to PIA Support (piasupport@va.gov) annually, or as needed.
» Steps to review PII holdings are:
• Remove less-active records to local storage.
• Transfer inactive records to an approved records offsite storage facility.
• Transfer permanent records to the National Archives.
• And destroy and document the destruction of records which have reached the term of their authorized retention period.
CIES SOP sets the following requirements: CIES VetsEZ Support Team will employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. Sanitization equipment must be on the NSA/CSS Evaluated Products List (EPL).
» All media for disposition must be recorded on VA0751.
» VA0751 must be reviewed for completeness and accuracy and signed by the individual performing the sanitization process, the System Owner, and Information System Security Officer prior to media disposition.
» A "Certificate of Destruction" provided by the nationally approved media disposition vendor conducting destruction must be kept with the associated VA0751 and maintained by the System Owner for three years.
» The implementation of media sanitization and disposition is defined under the following:
• Media Protection (MP)'s Media Sanitization,
• Knowledge Service's Security Controls Explorer
• Standard Operating Procedure Media Sanitization and Disposition
• National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88 Revision 1, Guidelines for Media Sanitization
• NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.
CIES is a transport mechanism and does not retain PII or other data internally.

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.*

CIES does not retain data long term. Data is stored only until data validation occurs at the VAMC or the CCP where a Consult is transmitted from a local VAMC. It is estimated that data remains within CIES for under 96 hours in extreme cases, for example a long holiday weekend. Once data is verified at the local VA medical center it is cleared from CIES system storage.

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?

CIES falls under the SORN for 79VA10 Veterans Health Information Systems and Technology Architecture (VistA) Records-VAhttps://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. CIES is a transport mechanism and does not store PII or other data internally. Each medical center follows the VA guidance for records retention of healthcare operations data.

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

CIES falls under the SORN for 79VA10 Veterans Health Information Systems and Technology Architecture (VistA) Records-VAhttps://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf\. CIES is a transport mechanism and does not store PII or other data internally. Each medical center follows the VA guidance for records retention of healthcare operations data.

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.
CIES falls under the SORN for 79VA10 Veterans Health Information Systems and Technology Architecture (VistA) Records-VAhttps://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. CIES is a transport mechanism and does not store PII or other data internally. Each medical center follows the VA guidance for records retention of healthcare operations data.

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.
CIES VetsEZ Support Team uses sample data for training and testing systems (Test/Development and Pre-Production). In some cases, while working with local VAMC administrators there may be situations where Production is used for implementation training and in these cases the local VAMC administrators will have access to their own facilities data being transmitted via CIES.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

Privacy Risk: ***The system collects, processes, and retains PII and PHI on Veterans and on Members of the Public, primarily Community Care Providers. Data is retained longer enough to validate it at the local medical center or by the CCP organization. This could be hours, but generally not longer than 96 hours (over the weekend). Once validated the data is no longer retained within CIES, the data is then added to the medical center VistA, VistA Imaging, or PACS system.***

Mitigation: ***CIES VetsEZ Support Team is responsible for conducting an initial evaluation of personally identifiable information (PII) holdings, via the PTA, and submitting the PTA to PIA Support (piasupport@va.gov) annually, or as needed. CIES Privacy SOP, sets the following requirements:***
» Steps to review PII holdings are:

• Remove less-active records to local storage.
• Transfer inactive records to an approved records offsite storage facility.
• Transfer permanent records to the National Archives.
• And destroy and document the destruction of records which have reached the term of their authorized retention period.

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?

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Health Administration	System Log files, sample clinical data that may contain Protected Health Information (PHI)	Patient identifier (VA and Community Partner potential), Consult Number (Referral Number), DOB, SSN	Internal VA network to/from VAEC Amazon GovCloud
Veterans Health Administration	DICOM Images and HL7	Patient identifier (VA and Community Partner potential),	Internal VA network to/from

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*
	Reports which may contain Protected Health Information (PHI)	Consult Number (Referral Number), DOB, SSN	VAEC Amazon GovCloud

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: ***The system collects, processes, and retains PII and PHI on Veterans and on Members of the Public, primarily Community Care Provider (CCP) organizations, which could be compromised. In accordance with CIES Privacy SOP, CIES VetsEZ Support Team works with local VAMC Department heads / Supervisors to require local VAMCs assign/review functional categories for users and ensure they have access to the information required to perform job duties. VAMC local Department heads / Supervisors are to discuss with staff the need to only access the minimum necessary PII to conduct their duties. Risk from privacy (disclosure, manipulation, etc.) is very low as only those with current Electronic Health Record Access will have access to this additional information.***

Mitigation: ***CIES VetsEZ Support Team is responsible for ensuring all internal data transmissions are in accordance with VA security requirements, and only that data necessary to be transmitted is sent. CIES VetsEZ Support Team will coordinate requirements with the Information System Security Officer and Privacy Officer, along with the Information System Owner.***

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.

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***
Community Care Services (VA)	***Patient care services***	***Social Security Number, Patient Identifier (VA and CCP organization), Date of Birth.***	***CIES falls under the SORN for 79VA10 Veterans Health Information Systems and Technology Architecture (VistA) Records***	***Port 443, 343***

Vaultara Flight Image Sharing Solution	***External patient care (imaging)***	***Social Security Number, Patient Identifier (VA and CCP organization), Date of Birth.***	***CIES falls under the SORN for 79VA10 Veterans Health Information Systems and Technology Architecture (VistA) Records***	***Port 443, 343***
Nuance PowerShare (COTS Vendor)	***Social Security Number, Patient Identifier (VA and CCP organization), Date of Birth.***	***Port 443, 343***	***Business Associate Agreement, Memorandum of Understanding – Interconnection Security Agreement (MOU-ISA)***	***Nuance PowerShare (COTS Vendor)***
ViTel Net vCareNterprise (referred to as vCARE) (COTS Vendor)	***Social Security Number, Patient Identifier (VA and CCP organization), Date of Birth.***	***Port 443, 343***	***Business Associate Agreement, Memorandum of Understanding – Interconnection Security Agreement (MOU-ISA)***	***ViTel Net vCareNterprise (referred to as vCARE) (COTS Vendor)***

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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

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

Follow the format below:

Privacy Risk: ***The system collects, processes, and retains PII and PHI on Veterans and on Members of the Public. Lack of documents such as the BAA, MOU, NDA, and other documents could result in personal and financial harm to the individuals impacted and adverse negative effect to the VA.***

Mitigation: ***CIES VetsEZ Support Team is responsible for ensuring all internal and external data sharing services are in accordance with VA security requirements. CIES VetsEZ Support Team will coordinate requirements with the Information System Security Officer and Privacy Officer, along with the Information System Owner. CIES VetsEZ Support Team includes the CIES eMASS System Steward who is responsible for drafting and coordination of MOUs and other documentation with the Information System Owner, Privacy Officer, Information System Security Officer, and other applicable individuals. In accordance with CIES Privacy SOP, A Statement of Work (SOW) or Performance Work Statement (PWS) will be written to establish privacy roles and responsibilities for contractors if they are required to have access to PHI/PII.***
» Information System Security Officer/Privacy Officer complete a Contract Security Checklist 6500.6 on all contracts to ensure that appropriate security and privacy requirements are included. The Privacy Officer determines if a Business Associate Agreement (BAA) is required or if a local/national BAA is already in place.
» A BAA is required if the business associate that will be performing a function on behalf of CIES VetsEZ Support Team or will be providing a service that involves the use or disclosure of PHI.
» Contractor/Service Providers are required to complete Talent Management Service (TMS) courses:
• Privacy and Information Security Awareness training & Rules of Behavior (ROB) VA10176
• Privacy & HIPAA VA10203

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.
Veterans enrolled and eligible to enroll for care, and caregivers receive a copy of the Notice of Privacy Practices (NOPP) every three years via mass mailing. The NOPP explains the collection and use of protected health information. and use of protected health information. and use of protected health information.

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.
CIES falls under the SORN for 79VA10 Veterans Health Information Systems and Technology Architecture (VistA) Records-VAhttps://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf).

Enter Major Application name here.

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 NOPP provides explanation of how VHA uses and discloses health information for treatment, payment, and health care operations.

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

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.
VHA requests information necessary to administer benefits to Veterans and other potential beneficiaries. While Veteran, patient or beneficiary may choose not to provide information to VHA, this may preclude the ability of VA to deliver the benefits due to those individuals or to verify their identity. Employees and VA contractors are required to provide the requested information to maintain employment and/or their affiliation with the VA.

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, individuals may request in writing a record restriction limiting the use of their information by filling out a written request. The request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-

out, no information on the individual is given out. Individuals can request further limitations on other disclosures. A Veteran, guardian or court appointed Power of Attorney can submit a request to the facility Privacy Officer to obtain inform

VHA permits individuals to give consent or agree to the collection or use of their personally identifiable information (PII) through the use of paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. In addition, information is collected verbally from individuals. If individuals are not willing to give information verbally then they are not required to do so. Individuals are made aware of when they must give consent when there is data collected about them through the VHA Notice of Privacy Practices and conversations with VHA employees. VA Forms are reviewed by VHA Central Office periodically to ensure compliance with various requirements including that Privacy Act Statements which are on forms that collect personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations where required. If the individual does not want to give consent, then they are not required to in most cases unless there is a statute or regulation that requests the collecting and then consent is not necessary but when legally required VHA obtains a specifically signed written authorization for each intended purpose from individuals prior to releasing, disclosing, or sharing PII and PHI.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: ***The system transmits and processes image related data but does not retain PII and PHI on Veterans and on Members of the Public. CIES system is not accessed directly by users (VA healthcare providers) the system connects imaging systems between VA and Community Care Providers imaging systems. CIES is an imaging transport system which transfers files from Community Care Providers who have been contracted for services to veterans. The risk to privacy (disclosure, manipulation, etc.) is very low as only a limited number of individuals with appropriate clearance have access.***

Mitigation: ***In accordance with CIES Privacy SOP, CIES VetsEZ Support Team and OIT provides effective notice to the public regarding its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII). CIES VetsEZ Support Team will coordinate requirements with the Information***

System Security Officer and Privacy Officer, along with the Information System Owner. CIES supports data processing for VistA and VistA Imaging and no additional data fields are within CIES which are not in those 2 systems.

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.***

CIES falls under the SORN for 79VA10 Veterans Health Information Systems and Technology Architecture (VistA) Records-VAhttps://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf).

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)?

CIES falls under the SORN for 79VA10 Veterans Health Information Systems and Technology Architecture (VistA) Records-VAhttps://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf).

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?

When requesting access to one's own records, patients are asked to complete VA Form 10-5345a: Individuals' Request for a Copy of their Own Health Information, which can be obtained from the medical center or online at http://www.va.gov/vaforms/medical/pdf/vha-10-5345a-fill.pdf. Veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the MyHealtheVet program, VA's online personal health record. More information about MyHealtheVet is available at https://www.myhealth.va.gov/index.html. In addition to the procedures discussed above, the SORNs listed in the Overview section of this PIA each address record access, redress, and correction. Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact Contract Officer Representative to obtain information 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.

VHA has a documented process for individuals to request inaccurate PII be corrected or amended and a process for review to determine if correction or amendment is appropriate. The policy complies with both the Privacy Act, VA regulations and the HIPAA Privacy Rule and is described in detail in VHA Directive 1605.01 Privacy and Release of Information. Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SORN. Every VHA Privacy Act SORN contains information on Contesting Record Procedure which informs the individual who to contact for redress. The VHA NOPP also informs individuals how to file an amendment request with VHA.

CIES VetsEZ Support Team has developed the Community Image Exchange (CIES) Privacy SOP, an individual may request amendment of a record pertaining to them contained in a specific VA system of records by mailing or delivering the request to the office concerned. The request must be in writing and must conform to the requirements in VA Handbook 6300.4. It must state the nature of the information in the record the individual believes to be inaccurate, irrelevant, untimely, or incomplete; why the record should be changed; and the amendment desired. The requester is advised of the title and address of the VA official who can assist in preparing the request to amend the record if assistance is desired. Within 10 business days, the requester is provided a written acknowledgement of receipt of the request and formal decisions to amend the record is provided within 30 days. CIES falls under the SORN for 79VA10 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA which places redress activities with the individual VAMC Health Informatics Management Services (HIMS) department at each VAMC. https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

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.
Right to Request Amendment of Health Information.
You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.
If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:
•File an appeal

•File a "Statement of Disagreement"
•Ask that your initial request for amendment accompany all future disclosures of the disputed health information
Information can also be obtained by contacting the facility Release of Information (ROI) office

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.
A formal redress process via the amendment process is available to all individuals.

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

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

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

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

Follow the format below:

Privacy Risk: ***The system collects, processes, and retains PII and PHI on Veterans and on Members of the Public. If inappropriate access is permitted or patients are not able to address changes to information in their medical records, it could result in personal and financial harm to the individuals impacted and adverse negative effect to the VA.***

Mitigation: ***CIES VetsEZ Support Team is responsible for ensuring all internal data transmissions are in accordance with VA security requirements, and only that data necessary to be transmitted is sent. CIES VetsEZ Support Team will coordinate requirements with the Information System Security Officer, Privacy Officer, along with the Information System Owner.***

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?
As documented previously, the only users with direct access to the CIES system is the System Administrator and Developer roles. This is accomplished following standardize VA electronic Permission Access System (ePAS) process. The Information System Owner or Contracting Officer Representative (COR) must approve all elevated access accounts.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?
There are no users from other agencies.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.
There are two account types within CIES. The first role is that of System Administrator, who duties includes installation of software on the VAEC Amazon GovCloud Virtual Machines (VMs) on their servers. The CIES VetsEZ Support Team System Administrator will also install vendor software onto the vendor gateways within the CIES boundary on the VAEC Amazon GovCloud environment. The second role is that of Developer, which are individuals who develop software for use with VistA, VistA Imaging, VIX, HDIG, and other servers.

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.
The CIES VetsEZ Support Team is the contractor support for the CIES system. All Project Management, System Administration, and Development efforts is provided under the Statement of Work (SOW) with VetsEZ. Support also includes Security and Privacy Compliance requirements, as well as System Steward duties in eMASS. The Statement of Work (SOW) or Performance Work Statement (PWS) will be written to establish privacy roles and responsibilities for contractors if they are required to have access to PHI/PII. A BAA is required if the business associate that will be performing a function on behalf of CIES VetsEZ

Support Team or will be providing a service that involves the use or disclosure of PHI. Contractor/Service Providers are required to complete Talent Management Service (TMS) courses: Privacy and Information Security Awareness training & Rules of Behavior (ROB) VA10176 and Privacy & HIPAA VA10203 The PO determines if a Business Associate Agreement (BAA) is required or if a local/national BAA is already in place. On July 10, 2023, the PO has approved the National BAA with Velocity Application, which includes the Vaultara Flight Image Sharing Solution. BAA with other vendors are pending.

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.
CIES will follow current VHA required privacy training requirements, including requirements for access to PHI which require users attend HIPAA Privacy Training course(s) based on their roles. CIES VetsEZ Support Team members must all complete this training.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* ***In Process***
2. *The System Security Plan Status Date:* ***October 30, 2023***
3. *The Authorization Status****: In Process***
4. *The Authorization Date:* ***In Process***
5. *The Authorization Termination Date:* ***N/A***
6. *The Risk Review Completion Date:* ***In Process***
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* ***Confidentiality = Moderate, Integrity = Moderate, Availability = Low, Overall Security Categorization = 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.***
In Process, anticipated system IOC date is March 30, 2024.

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)*

Yes, CIES is housed within the VAEC Amazon GovCloud, a VA-managed FedRAMP authorized Cloud Service Provider. CIES will be a Platform as a Service (PaaS) providing access to DICOM images and HL7 reports using vendor COTS products.

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.*

Not Applicable.

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.

Not Applicable.

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.

Not Applicable.

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).

Not Applicable.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

KAMILAH M. JACKSON 105810

Digitally signed by KAMILAH M. JACKSON 105810
Date: 2024.01.17 13:00:00 -05'00'

Privacy Officer, Kamilah Jackson

RICHARD ALOMAR-LOUBRIEL

Digitally signed by RICHARD ALOMAR-LOUBRIEL
Date: 2023.12.06 09:58:26 -04'00'

Information System Security Officer, Richard Alomar-Loubriel

JOHN DI LORENZO

Digitally signed by JOHN DI LORENZO
Date: 2023.11.21 13:02:09 -07'00'

Information System Owner, John Di Lorenzo

APPENDIX A-6.1

Community Image Exchange Services (CIES) adheres to the standard VHA Privacy Notice under the SORN for 79VA10 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA.

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

VHA Notice of Privacy Practices

https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices