Privacy Impact Assessment for the VA IT System called:

Infrastructure as a Managed Service (IaaMS)

VA Information Technology Operations and Service (ITOPS) Veterans Health Administration

Date PIA submitted for review:

July 12, 2022

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	787-696- 4091
Information System Owner	Scott Price	Scott.price@va.gov	937-972-1665

Abstract

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

The Infrastructure as a Managed Service (IaaMS) project is to expand Vista Imaging (VI) storage by an additional 220+ petabytes of capacity to approximately 300 VA facilities by replacing onsite hardware and modifying how the system stores data by moving the disaster recovery copy of all patient images storage to the VA's Enterprise Cloud (VAEC) cloud.

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

VA Information Technology Operations and Service (ITOPS), Infrastructure as a Managed Service (IaaMS) solution is a storage and computer infrastructure deployed at facilities across the United States and abroad. All hardware, software, and professional services provided as part of this program will be utilized to replace existing storage and compute platforms residing at facilities across the United States and abroad as they reach end of life (EOL) status. The IaaMS solution will initially deploy a Veterans Health Information Systems and Technology Architecture (VistA) Imaging (VI) storage systems solution to VA facilities. The initial deployment will replace legacy VI storage systems located at 158 facilities. The existing VI infrastructure stores approximately 10 billion medical images and 40 billion total files using over 28 petabytes (PB). Under the IaaMS solution, VA shall replace the VI architecture with approximately 11 PB of on-premises storage and 11PB of IaaMS VI cloud disaster recovery repository to be hosted in Amazon Web Services (AWS) under VA's Enterprise Cloud (VAEC), with the remainder

eliminated through use of data efficiency technologies. Following the VI initial deployment, it is anticipated that the IaaMS solution shall expand by an additional 220+ PB of capacity over the Period of Performance (PoP). Expansion shall be provided via optional tasks for file, block, and object storage using both minimally managed and fully managed services and presented using a variety of storage performance tiers. Additional VA storage and compute workloads such as CVI (facility file shares), TBE (Tapeless Backup Encryption), and Storage on Demand (SOD) have been identified as potential follow on IaaMS workloads beyond the initial VistA Imaging deployment.

The IaaMS solution is the primary storage component of the VHA VI system. The VHA VI system collects, processes, and/or retains the information of over one million Veterans, contractors and VA employee information, and encompasses the both the facility level (Tier One) and the second-tier repository of the data which establishes a second instance of the data to ensure redundancy It is important to note that as an FDA approved system, changes to the Vista Imaging require a rigorous approval process. Therefore, there is little to no variation in the technical footprint of the Vista Imaging instances nationwide. The systems at both the tier one and tier two levels are identical. The type of data the system collects, and processes varies and is dependent on the role of the affected individual. For instance, Veteran data is usually in the form of health images and supporting information and therefore consists of PHI and PII data, whereas employee and contractor information is usually in the form of administrative data based on their role in maintaining, processing or securing data in the system, which may also consist of PII data. The system is a two-tier system that meets data redundancy requirements but is completely contained within VA and part of an internal Cloud system. VistA Imaging utilizes a virtual private cloud within VAEC for additional storage/disaster recovery.

Legal authority to operate IaaMS is the primary data storage for Vista Imaging (VI) and its support of VistA. Legal authority to operate follows as VistA. VistA has a Systems of Records Notice: 79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA 12/23/2020 Web link: Current SORN List (va.gov) . SOR Number: 79VA10. Link to SORN: https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf.

Completion of this PIA will not result in circumstances that will require change in business processes or technology as this modernization allows for continued use of as is business process and update of back-end storage.

As IaaMS is the primary storage and backup data solution for Vista and Vista's imaging, its current SORN covers on-premises VA data storage as well as modernization using VA Enterprise Cloud storage (VAEC) storage.

The boundary comprises assets located at the VA medical centers listed here:

Bedford, MA	Salisbury, NC	Hines, IL	Eastern Colorado HCS
Boston HCS	Atlanta, GA	Iron Mountain, MI	Grand Junction, CO
Connecticut HCS	Augusta, GA	Madison, WI	Montana HCS
Manchester, NH	Birmingham, AL	Milwaukee, WI	Salt Lake City, UT
Northampton, MA	Central Alabama HCS	North Chicago, IL	Sheridan, WY
Providence, RI	Charleston, SC	Tomah, WI	Anchorage, AK
Togus, ME	Columbia, SC	Columbia, MO	Boise, ID

White River Junction, VT	Dublin, GA	Kansas City, MO	Portland, OR
Albany, NY	Tuscaloosa, AL	Leavenworth, KS	Puget Sound HCS
Bath, NY	Bay Pines CIO Test	Marion, IL	Roseburg, OR
Canandaigua, NY	Bay Pines, FL	Poplar Bluff, MO	Spokane, WA
Syracuse, NY	Lake City VA Medical Center	St. Louis, MO	Walla Walla, WA
Upstate NY HCS	Miami, FL	Topeka, KS	White City OR
Bronx, NY	N. Florida/S. Georgia HCS	Wichita, KS	Fresno, CA
Hudson Valley HCS	Orlando, FL	Alexandria, LA	Honolulu, HI
NY HCS	San Juan, PR	Biloxi, MS	Manila, PI
New Jersey HCS	Tampa, FL	Fayetteville, AR	Northern California HCS
Northport, NY	West Palm Beach, FL	Houston, TX	Palo Alto HCS
Altoona, PA	Huntington, WV	Jackson, MS	Reno, NV
Butler, PA	Lexington, KY	Little Rock, AR	San Francisco, CA
Clarksburg, WV	Lexington, KY -CDD	Muskogee, OK	Las Vegas, NV
Coatesville, PA	Louisville, KY	New Orleans, LA	Loma Linda, CA
Erie, PA	Memphis, TN	Oklahoma City, OK	Long Beach, CA
Lebanon, PA	Mountain Home, TN	Pensacola, FL	San Diego, CA
Philadelphia, PA	Tennessee Valley HCS	Shreveport, LA	West Los Angeles, CA
Pittsburgh HCS	Chillicothe, OH	Central Texas HCS	Black Hills HCS
Wilkes Barre, PA	Cincinnati, OH	North Texas HCS	Central Iowa HCS
Wilmington, DE	Cleveland, OH	South Texas HCS	Central Plains HCS
Martinsburg, WV	Columbus, OH	Valley Coastal Bend HCS	Fargo, ND
Maryland HCS	Dayton, OH	Albuquerque, NM	Grand Island, NE
Washington, DC	Ann Arbor, MI	Amarillo, TX	Iowa City, IA
Asheville, NC	Big Spring, TX	Tucson, AZ	VAEC
Beckley, WV	El Paso, TX	Lincoln, NE	Billings, MT CBOC
Durham, NC	Phoenix, AZ	Minneapolis, MN	Cheyenne, WY
Fayetteville, NC	Prescott, AZ	Sioux Falls, SD	Battle Creek, MI
Hampton, VA	Northern Indiana HCS	St. Cloud, MN	Danville, IL
Richmond, VA	Saginaw, MI	Detroit, MI	
Salem, VA	Chicago, IL (Westside)	Indianapolis, IN	

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☒ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☒ Personal Fax Number
- ☒ Personal Email Address
- ☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial 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
- ☐ Gender
- ☐ Integration Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Unique Identifying Information (list below)

Radiology Number (RAD)
Consult Number (CON)
Study Number
X-ray Technician Name
Facility Name
Reason for Image
What Type of Study

PII Mapping of Components

Infrastructure as a Managed Service (IaaMS) consists of 4 key components/workflows (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by IaaMS and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Tier I and Tier 2 Storage	Yes	Yes	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), Health Insurance Beneficiary Numbers Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Name, Reason for Image, What Type of Study	Many medical image modalities embed patient information within the image output.	Housed in secure VA Health facilities/ VAEC AWS and accessible only by authenticated users.

Converged Infrastructure (CVI)	Yes	Yes	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), Health Insurance Beneficiary Numbers Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Name, Reason for Image, What Type of Study	Many medical image modalities embed patient information within the image output.	Housed in secure VA Health facilities/ VAEC AWS and accessible only by authenticated users.

Storage On Demand (SOD)	Yes	Yes	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), Health Insurance Beneficiary Numbers Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Name, Reason for Image, What Type of Study	Many medical image modalities embed patient information within the image output.	Housed in secure VA Health facilities/ VAEC AWS and accessible only by authenticated users.

Tape Backup Encryption (TBE)	Yes	Yes	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), Health Insurance Beneficiary Numbers Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Name, Reason for Image, What Type of Study	Many medical image modalities embed patient informatio n within the image output.	Housed in secure VA Health facilities/ VAEC AWS and accessible only by authenticat ed users.

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.

IaaMS is the storage component of Vista Imaging (VI). As the primary repository and delivery system for patient health imaging in VA, the Vista Imaging systems' principal source of data are the clinicians and the intake systems they utilize to prepare those artifacts such as Magnetic Resonance Imaging (MRI) systems, Sonography (Ultrasound) and X-Ray systems. However, the VI system is not limited to only imaging artifacts but also contains ancillary supporting artifacts and information that come from varied data sources such as scanning devices and interfaces with other VA applications and systems. The primary rationale for the collection of all Vista Imaging data is to ensure the contextual storage and delivery Veteran healthcare information. In addition to the primary data, the health images, ancillary data from multiple input modalities are collected to contextualize patient data to ensure clinicians have access to the complete medical picture when managing Veteran healthcare. This ancillary data may take different forms such as image representations of standard VA forms as well as supporting medical documentation.

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.

IaaMS shares information from VistA.

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

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

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

IaaMS as primary storage for VistA, integrity is maintained using the checksum hash validation process with the Dell SRM migration tool. IaaMS collects logs to validate the integrity of the original file when it lands on IaaMS. On stored Cisco Hyperflex (HX) data, all distributed objects in the cluster are addressable by checksum data integrity validation.

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

IaaMS is the primary data storage for Vista Imaging (VI) and its support of VistA. The National Vista Imaging System and facility entities operate under the authority of Veterans' Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a), 45 CFR Part 160 - GENERAL ADMINISTRATIVE REQUIREMENTS, 21 CFR 803. Medical Device

Reporting, and 21 CFR 807. Market Clearance

VHA System of Records Notice: Patient Medical Records-VA, SORN 24VA10A7, in the Federal Register and online.
Link to SORN: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf2)

VHA System of Record Notice (VA SORN) Veterans Health Information System and Technology Architecture (VISTA) - VA, SORN 79VA10A7, in the Federal Register and online.
Link to SORN: 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.

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: If the data were accessed by an unauthorized individual or otherwise breached, serious harm, embarrassment or even identity theft may result.

Mitigation: Veterans Health Administration (VHA), National Vista Imaging System facilities deploy extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of all employees and contractors throughout the nation. The National Vista Imaging System security measures include 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, planning and maintenance. Vista Imaging is subjected to routine audit for compliance with VA 6500, ensuring the systems maintains the proper controls for protecting the data under its purview.

Data from DoD is collected from the patient's electronic health record and transmitted via the Medical Community of Interest (MEDCOI), an enterprise Multi-Protocol Label Switched Layer 3 Virtual Private Network (VPN) that provides DoD and VA a secure logical medical enclave to support the delivery of healthcare by both Departments. Data passed between MEDCOI Enterprise Gateway and VA is required to use encryption mechanisms approved by Federal Information Processing Standards Publication 140-2.

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.

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

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The primary purpose of the Vista Imaging system is the storage and presentation of patient medical information and the supporting artifacts. The system also stores administrative data on those entrusted to use, manage and support the system. Vista Imaging itself does not employ tools that perform functions with the intended purpose of augmenting data files or databases.

Simple functions to search and retrieve records are available to the user but the system does not perform analytical functions that produce relevant health outputs that must be stored in compliance with US law. Vista Imaging is simply a data storage and retrieval system, not an analytical system.

Tools and applications used to analyze data will vary from facility to facility. Please reference the individuals Privacy Impact Assessments for each facility to learn more.
http://www.privacy.va.gov/privacy_impact_assessment.asp

2.3 How is the information in the system secured?

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

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

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

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

Secure Communication (SC) of the PII/PHI VistA data managed by the IaaMS storage solution is provided by Federal Information Processing Standards (FIPS) 140-2 level data encryption during transit and at rest.

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

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

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

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

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

IaaMS storage solution is the primary data storage for the VistA Imaging data. Access to the Vista Imaging data is determined at the facility and is roles-based. Facilities are required by VA 6500 to implement process controls that ensure that access to VA systems is strictly controlled and regulated based on job requirements, these controls include the those governing the approval process for granting access as well as those that track and monitor access. Ultimately the Information System Owner (ISO) and facility leadership are responsible for ensuring that the controls are documented, implemented and tracked. VA works with the Office of the Inspector General (OIG) to conduct annual audits to ensure that these controls are in place and followed. Random, unscheduled audits of facility and national processes may be conducted at any time to also ensure compliance.

Additionally, there are controls in place to ensure that the information is handled in accordance with the uses described above include mandatory online information security and HIPAA training; face-to-face training for all incoming employees conducted by the Information Security Officer and Privacy Officer; regular audits of individuals accessing sensitive information; and formal rounds during which personal examination of all areas within the facility to ensure information is being appropriately used and controlled.

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

Data Elements:

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), Health Insurance Beneficiary Numbers Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Name, Reason for Image, What Type of
Study

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

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

IaaMs is the storage and transfer of data, the official records are maintained in VistA for 75 years after the last episode of care.

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.
When managing, and maintaining VA data and records, All healthcare facilities will follow the guidelines established in the VA and NARA-approved Veteran Health Administration Record Control Schedule (RCS)10-1 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf). Per the VHA Records Management Staff official records are maintained in VistA for 75 years after the last episode of care.

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

Records in this system are maintained in accordance with VHA Records Retention Schedule (RCS 10-1) under Section 6000.2 Electronic Health Records (EHR) 75 years after the last episode of care.

VA Records management procedures are addressed in VA Handbook 6300.1
https://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=475&FType=2

Temporary paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371,
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=8310

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are disposed of in accordance with VA Directive 6500. https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=932&FType=2 and OIT-OIS SOP MP-6-Electronic Media Sanitization procedures.

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

The National Vista Imaging team utilizes de-identified test patient accounts for training purposes and all PII/SPI information is redacted when doing research.

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

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

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

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

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

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: There is an increased risk to patient privacy when records are maintained longer than authorized or necessary.

Mitigation: In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed in VI is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is available for only as long as necessary, reducing its exposure to malicious attack. Vista Imaging will continue to employ security controls in compliance with VA Handbook 6500 that reduce the threat of data breach as technology capabilities advance.

Please review the Privacy Impact Assessments (PIAs) for the facilities you are seeking information regarding. PIAs are available online at: http://www.privacy.va.gov/privacy_impact_assessment.asp https://www.oprm.va.gov/privacy/pia.aspx

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?
NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

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

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

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

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
VHA	***VistA. IaaMS is the primary storage and DR for VistA. Clinicians access VistA for patient care.***	***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), Health Insurance Beneficiary Numbers Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Name, Reason for Image, What Type of Study***	***Internal VA traffic only utilizing Hypertext Transfer Protocol Secure (HTTPS) over Secure Sockets Layer (SSL)/Transport Layer Security TLS.***
VHA	***Vista Imaging (VI). IaaMS is the primary***	***Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Phone Number(s),***	***Internal VA traffic only utilizing Hypertext Transfer Protocol Secure (HTTPS) over***

	storage and DR for VistA. Clinicians access VistA for patient care.	***Personal Fax Number, Personal Email Address, Emergency Contact Information (Name, Phone Number, etc. of a different individual), Health Insurance Beneficiary Numbers Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Name, Reason for Image, What Type of Study***	***Secure Sockets Layer (SSL)/Transport Layer Security TLS.***
VHA	***Joint Legacy Viewer (JLV). IaaMS is the primary storage and DR for VistA. Clinicians access VistA for patient care.***	***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), Health Insurance Beneficiary Numbers Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Name, Reason for Image, What Type of Study***	***Internal VA traffic only utilizing Hypertext Transfer Protocol Secure (HTTPS) over Secure Sockets Layer (SSL)/Transport Layer Security TLS.***
VHA	***Magnetic Resonanc e Imaging (MRI) systems.***	***Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Phone Number(s),***	***Internal VA traffic only utilizing Hypertext Transfer Protocol***

	IaaMS is the primary storage and DR for VistA. Clinicians access VistA for patient care.	***Personal Fax Number, Personal Email Address, Emergency Contact Information (Name, Phone Number, etc. of a different individual), Health Insurance Beneficiary Numbers Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Name, Reason for Image, What Type of Study***	***Secure (HTTPS) over Secure Sockets Layer (SSL)/Transport Layer Security TLS.***
VHA	***Sonography (Ultrasound). IaaMS is the primary storage and DR for VistA. Clinicians access VistA for patient care.***	***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), Health Insurance Beneficiary Numbers Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Name, Reason for Image, What Type of Study***	***Internal VA traffic only utilizing Hypertext Transfer Protocol Secure (HTTPS) over Secure Sockets Layer (SSL)/Transport Layer Security TLS.***

VHA	***X-Ray systems. IaaMS is the primary storage and DR for VistA. Clinicians access VistA for patient care.***	***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), Health Insurance Beneficiary Numbers Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Name, Reason for Image, What Type of Study***	***Internal VA traffic only utilizing Hypertext Transfer Protocol Secure (HTTPS) over Secure Sockets Layer (SSL)/Transport Layer Security TLS.***
VHA	***CVI (facility file shares). IaaMS is the primary storage and DR for VistA. Clinicians access VistA for patient care.***	***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), Health Insurance Beneficiary Numbers Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Name,***	***Internal VA traffic only utilizing Hypertext Transfer Protocol Secure (HTTPS) over Secure Sockets Layer (SSL)/Transport Layer Security TLS.***

		Reason for Image, What Type of Study	
VHA	***TBE (Tapeless Backup Encryption). IaaMS is the primary storage and DR for VistA. Clinicians access VistA for patient care.***	***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), Health Insurance Beneficiary Numbers Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Name, Reason for Image, What Type of Study***	***Internal VA traffic only utilizing Hypertext Transfer Protocol Secure (HTTPS) over Secure Sockets Layer (SSL)/Transport Layer Security TLS.***
VHA	***Storage on Demand (SOD). IaaMS is the primary storage and DR for VistA. Clinicians access VistA for patient care.***	***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), Health Insurance Beneficiary Numbers Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Radiology***	***Internal VA traffic only utilizing Hypertext Transfer Protocol Secure (HTTPS) over Secure Sockets Layer (SSL)/Transport Layer Security TLS.***

		Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Name, Reason for Image, What Type of Study	

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: However, there is a risk that the data could be shared with an inappropriate VA organization or institution which would have a potential impact on privacy. The scale of the impact would be dependent on the level of breach associated with risk realization.

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, planning and maintenance.

Electronic Permission Access System (ePAS) mitigates the risk of inadvertently sharing or disclosing information by assigning access permissions based on need to know.

The use of a Personal Identity Verification (PIV) card is implemented. This ensures the identity of the user by requiring two-factor authentication.

Microsoft Outlook is also another tool that is used to share internal information within the organization. Risks are mitigated by using encryption methods to share sensitive information within the organization.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>
Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

<u>Privacy Risk:</u> N/A

<u>Mitigation:</u> N/A

Section 6. Notice

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

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

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

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

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

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090 is a document which explains the collection and use of protected health information to individuals interacting with VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans.

Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis.

The Department of Veterans Affairs provides additional notice of this system by publishing 2 System of Record Notices (SORNs):
The VA System of Record Notice (VA SORN) Veterans Health Information System and Technology Architecture (VISTA) - VA, SORN 79VA10A7, in the Federal Register and online. An online copy of the SORN can be found at:
https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10A7, in the Federal Register and Online. An online copy of the SORN can be found at:
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

This Privacy Impact Assessment (PIA) also serves as notice of the National Vista Imaging System. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

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

Per content from the VistA Imaging (VI) Privacy Impact Assessment (PIA), the Veterans' Health Administration (VHA) requests only 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 those individuals, Employees and VA contractors are required to provide the requested information to maintain employment and/or their affiliation with the VA.

VHA Directive 1605.01 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

Additionally, the NOPP outlines instances when VA may use their information without their consent as captured at the point of care.

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 information.

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.

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:** There is a risk that an individual may not receive the NOPP that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration prior to providing the information to the VHA.
>
> **Mitigation:** This risk is mitigated by the common practice of providing the VHA Notice of Privacy Practice (NOPP) when Veterans apply for benefits and mailed notices every 3 years. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

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.

This risk is mitigated by the common practice of providing the VHA Notice of Privacy Practice (NOPP) when Veterans apply for benefits and mailed notices every 3 years. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

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
.
Additionally, 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.

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.

This risk is mitigated by the common practice of providing the VHA Notice of Privacy Practice (NOPP) when Veterans apply for benefits and mailed notices every 3 years. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

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 contact information on Contesting Record Procedure which informs the individual who to contact for redress. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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.

This risk is mitigated by the common practice of providing the VHA Notice of Privacy Practice (NOPP) when Veterans apply for benefits and mailed notices every 3 years. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

Veterans are informed of the amendment process by many resources to include the Notice of Privacy Practice (NOPP) which states:

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

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

This risk is mitigated by the common practice of providing the VHA Notice of Privacy Practice (NOPP) when Veterans apply for benefits and mailed notices every 3 years. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

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.

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

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

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

Follow the format below:

> **Privacy Risk:** There is a risk that individuals whose records contain incorrect information may not receive notification of appointments prescription medications, or test results. Furthermore, incorrect information in a health record could result in improper diagnosis and treatments. Additionally, there is a risk that a Veteran may not know how to obtain access to their records or how to request corrections to their records.
>
> **Mitigation:** VHA mitigates the risk of incorrect information in an individual's records by authenticating information when possible, using the resources discussed in question 1.5. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.
> • VHA staffs Release of Information (ROI) offices at facilities to assist Veterans with obtaining access to their medical records and other records containing personal information.

• The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans
remote access to their medical records. The Veteran must enroll to obtain access to all the available features.
• In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

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

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

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

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

Access to each VI facility working and storage areas is restricted to VA employees who must complete both the VHA Privacy and HIPAA Focused training and Information Security training. Specified access is granted based on the employee's functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information Security Officer (ISO), local Chief Information Officer (CIO), System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information.

Access is requested per National Vista Imaging System policies utilizing Electronic Permission Access System (ePAS). Users submit access requests based on need to know and job duties.
Supervisor, ISO and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes. Once access is granted, individuals can log into the system(s) through dual authentication, i.e., a PIV card with a complex password combination. Once inside the system, individuals are authorized to access information on a need-to-know basis.
Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel.

Access to computer rooms at VI facilities and regional data processing centers is generally limited by

appropriate locking devices and restricted to authorized VA employees and vendor personnel. Automated Data Processing (ADP) peripheral devices are placed in secure areas (areas that are locked or have limited access) or are otherwise protected. Information that is downloaded from VistA and maintained on laptops and other approved government equipment is afforded similar storage and access protections as the data that is maintained in the original files. Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes. Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection at the health care facility, or an OIG office location remote from the health care facility, is controlled in the same manner.

Information downloaded from VistA and maintained by the OIG headquarters and Field Offices on automated storage media is secured in storage areas for facilities to which only OIG staff have access. Paper documents are similarly secured. Access to paper documents and information on automated storage media is limited to OIG employees who have a need for the information in the performance of their official duties. Access to information stored on automated storage media is controlled by individually unique passwords/codes.

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.

Contractors will have access to the system and the PII. Contracts are reviewed based on the contract guidelines by the appropriate contract authority (i.e., COR, Contracting Officer, Contract Review Committee).

Per specific contract guidelines, contractors can have access to the system only after completing mandatory information security and privacy training, VHA Privacy and HIPAA Focused training as well as the appropriate background investigation to include fingerprinting. Certification that this training has been completed by all contractors must be provided to the VHA employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy.
VA IaaMS Peraton staff and other supporting contractors have active Business Associate Agreements (BAA) and signed Non-Disclosure Agreements (NDA) that cover all staff involved in the deployment and maintenance of the IaaMS solution and VA data.

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

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

All VA employees and contractors who have access to VA computers must complete the onboarding and annual mandatory privacy and information security training. In addition, all employees who interact with patient sensitive medical information must complete the VA mandated VHA Privacy and HIPAA Focused training. Finally, all new employees receive training by the facility Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officer also perform subject specific trainings on an as needed basis.

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

If Yes, provide:

1. *The Security Plan Status,* Approved
2. *The Security Plan Status Date,* December 29, 2021
3. *The Authorization Status,* Authorization to Operate (ATO)
4. *The Authorization Date,* December 29, 2021
5. *The Authorization Termination Date,* December 27, 2022
6. *The Risk Review Completion Date,* December 29, 2021
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).* High

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

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

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

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.

IaaMS is the storage solution for VistA Imaging (VI). VistA Imaging does utilize VAEC AWS GovCloud storage. It has a FedRAMP high provisional ATO. It utilizes IaaS as service model.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

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

N/A

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

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

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

N/A

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

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

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

N/A

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

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

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

KAMILAH M. JACKSON 105810

Digitally signed by KAMILAH M. JACKSON 105810
Date: 2022.08.08 13:32:10 -04'00'

Privacy Officer, Kamilah Jackson

RICHARD ALOMAR-LOUBRIEL 139039

Digitally signed by RICHARD ALOMAR-LOUBRIEL 139039
Date: 2022.08.08 13:53:49 -04'00'

Information Systems Security Officer, Richard Alomar- Loubriel

Information Systems Owner, Scott Price

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).

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090 is a document which explains the collection and use of protected health information to individuals interacting with VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans.

Veteran Affairs Privacy Impact Assessment website: https://www.oprm.va.gov/privacy/pia.aspx

Veteran Affairs Form 10-5345a, Individuals Request for a Copy of Their Own Health Information, https://www.va.gov/vaforms/medical/pdf/VHA%20Form%2010-5345a%20Fill-revision.pdf

Veteran Affairs Form 10-5345, Request for and Authorization to Release Health Information, https://www.va.gov/vaforms/medical/pdf/VA_Form_10-5345.pdf

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