Privacy Impact Assessment for the VA IT System called:

VistA Imaging

Clinical Imaging, Health Information Operations (HIO), Infrastructure Operations

Veterans Health Administration

eMASS ID 1109

Date PIA submitted for review:

17 June 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy katz-johnson	Nancy.katz-johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Tristan Carroll	Tristan.carroll@va.gov	(210) 617-5300
Information System Owner	Larry Brown	Larry.brown5@va.gov	(941) 408-5576

Abstract

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

Vista Imaging (also referred to as VI) is the primary VA medical system for the collection, storing and presentation of VA's Medical Imaging artifacts and associated data. It is a critical VA system in the delivery of Veteran health as clinicians use the system daily as a tool to diagnose and treat veteran health issues. The Food and Drug Administration has classified the VistA Imaging software as a medical device. The use of VistA Imaging in a clinical setting is subject to the CFR (Code of Federal Regulations) Title 21 Part 820. The main features of the VistA Imaging system are:

Capturing clinical images, scanned documents, motion video, and other non-textual data files and making them part of the patient's electronic health record.

Delivering the multimedia component of the patient record to the clinician's desktop in an integrated, timely and accurate manner.

Enabling image sharing between VA hospitals and facilities, as well as the DoD.

Providing image data from specialties such as: cardiology, pulmonary and gastrointestinal medicine, pathology, radiology, surgery, dermatology, ophthalmology, hematology, radiotherapy, nuclear medicine, and others.

Providing a framework for image file storage, management, and retrieval.

Facilitating interoperability between VistA and commercial PACS using HL7 and DICOM standards and the IHE technical framework.

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?

VistA Imaging/OIT, DSO, SPM, Health, Clinical Services, Diagnostics

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 Veteran's Health Administration Vista Imaging (VI) system is a VA enterprise health system that operates under the authority of Veterans' Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), and Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, §7301(a). Vista Imaging as a technology system is owned and maintained by Clinical Imaging Support staff, a subdivision of Health Information Operations in Information Operations (IO) within the VA Office of Information and Technology (OI&T). As the system is a medical device, the data collected, stored and processed by the system is owned by the Veterans Health

Administration (VHA). While the Veteran is the ultimate benefactor of the Vista Imaging system as the recipient of the healthcare the system facilitates, the primary user/consumer community of the system is the VA clinicians delivering that healthcare. VI (e.g. servers, workstations, laptops, printers, commercial-off-the-shelf applications) supports mission-critical and other systems necessary to conduct day-to-day operations within the Veterans Health Administration by providing access to clinical images and supporting data used in the provisioning of patient care. The national VI boundary includes all hardware and software assets in VA that are dedicated to the support of the Vista Imaging system, including but not limited to servers, operating systems, application software, storage devices, system intake devices and networking devices. 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. VistA Imaging utilizes a virtual private cloud within VAEC for additional storage/disaster recovery. The Veteran's Health Administration Vista Imaging (VI) system is a VA enterprise health system that operates under the authority of Veterans' Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), and Veterans Health Administration Organization

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

VA Radiology Service

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?

Over one million plus VA patients.

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

Clinical images for the purpose of medical diagnosis and treatment.

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

VistA Imaging is comprised of the following applications: Capture, Display for MUSEAPII3 and Pre-MUSEAPI3, ISI Rad, Legacy DICOM Gateway, HDIG (Hybrid DICOM Gateway), Background Processor, VIX, Importer (VI DICOM Importer), Image Viewer. Importer (VI DICOM Importer), Image Viewer.

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?

1. The national VI boundary includes all hardware and software assets in VA that are dedicated to the support of the Vista Imaging system, including but not limited to servers, operating systems, application software, storage devices, system intake devices and networking devices.
2. 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.

3. 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	

3. Legal Authority and SORN

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

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
- 21 CFR 807. Market Clearance

Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code)
- 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).
- SORN 24VA10A7 Patient Medical Records – VA 2020-21426.pdf (govinfo.gov)
- SORN 79VA10/85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.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?

Yes

4. System Changes

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

No changes to business processes required.

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

No technology changes required.

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
☒ 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:
Radiology Number (RAD)
Consult Number (CON)
Study Number
X-ray Technician Name
Facility Name
Reason for Image
What Type of Study
Clinical images
Scanned documents
Motion video, and other non-textual data files.
Patient data
Patient data locations
DICOM images
Benefits
Clinical images
Scanned documents
Motion video
Other non-textual data files
Claims Decision
DD-214
System Log files
Cache log
Text files

PII Mapping of Components (Servers/Database)

VistA Imaging consists of 15 key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VistA Imaging 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. The first table of 3.9 in the PTA should be used to answer this question.

Occupational, Education, Medical)

Internal Components Table

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
Vista (on-prem)	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, Other Unique Identifying Information (list below); Radiology Number	Many medical image modalities embed patient information within the image output.	Housed in secure VA Health facilities and accessible only by authenticated users

			(RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Clinical images, scanned documents, motion video, and other non-textual data files. Patient data, Patient data locations, DICOM images, Benefits Name, Reason for Image, What Type of Study		
Bio-Med (on-prem)	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	To identify with patient medical record	Housed in secure VA Health facilities and accessible only by authenticated users

			Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Other Unique Identifying Information (list below); Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Clinical images, scanned documents, motion video, and other non-textual data files. Patient data, Patient data locations, DICOM images, Benefits Name, Reason for Image, What Type of Study		
Image Capture (on-prem)	Yes	Yes	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address,	Temporarily Stored	Housed in secure VA Health facilities and accessible only by authenticated users

			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, Other Unique Identifying Information (list below); Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Clinical images, scanned documents, motion video, and other non-textual data files. Patient data, Patient		

			data locations, DICOM images, Benefits Name, Reason for Image, What Type of Study		
MyHealtheVet	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, Other Unique Identifying Information (list below); Radiology	Temporarily Stored	Housed in secure VA Health facilities and accessible only by authenticated users

			Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Clinical images, scanned documents, motion video, and other non-textual data files. Patient data, Patient data locations, DICOM images, Benefits Name, Reason for Image, What Type of Study		
Embedded Fragment Registry (EFR) (on-prem)	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	Temporarily Stored	Housed in secure VA Health facilities and accessible only by authenticated users

			Numbers Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Other Unique Identifying Information (list below); Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Clinical images, scanned documents, motion video, and other non-textual data files. Patient data, Patient data locations, DICOM images, Benefits Name, Reason for Image, What Type of Study		
RefDoc (on-prem)	Yes	Yes	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing	Temporarily Stored	Housed in secure VA Health facilities and accessible only by authenticated users

			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, Other Unique Identifying Information (list below); Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Clinical images, scanned documents, motion video, and other non-textual data files. Patient		

			data, Patient data locations, DICOM images, Benefits Name, Reason for Image, What Type of Study		
After Visit Summary (AWS) (on-prem)	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, Other Unique Identifying Information (list below);	Temporarily Stored	Housed in secure VA Health facilities and accessible only by authenticated users

			Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Clinical images, scanned documents, motion video, and other non-textual data files. Patient data, Patient data locations, DICOM images, Benefits Name, Reason for Image, What Type of Study		
EHRM TeleReader Service (on-prem)	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	Temporarily Stored	Housed in secure VA Health facilities and accessible only by authenticated users

			Beneficiary Numbers Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Other Unique Identifying Information (list below); Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Clinical images, scanned documents, motion video, and other non-textual data files. Patient data, Patient data locations, DICOM images, Benefits Name, Reason for Image, What Type of Study		
IaaMS (Cloud)	Yes	Yes	Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal	Storage	Housed in secure VA Health facilities and accessible only by authenticated users

			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, Other Unique Identifying Information (list below); Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Clinical images, scanned documents, motion video, and other non-textual data		

			files. Patient data, Patient data locations, DICOM images, Benefits Name, Reason for Image, What Type of Study		
DSS Enterprise (DocManager Vista Scanning & Indexing System) (on-prem)	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, Other Unique Identifying Information	Temporarily Stored	Housed in secure VA Health facilities and accessible only by authenticated users

			(list below); Radiology Number (RAD), Consult Number (CON), Study Number, X-ray Technician Name, Facility Clinical images, scanned documents, motion video, and other non-textual data files. Patient data, Patient data locations, DICOM images, Benefits Name, Reason for Image, What Type of Study		

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?

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.

1.2b 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.

Information from other sources is not required.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

System does not create information.

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?

Collects information from individuals and/or received through electronic transmission from identified systems.

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?

Information collected from individuals is collected verbally in interviews and conversations with VA medical and administrative staff, in writing (such as on VA Form 10-5345, Request For and Authorization To Release Medical Records Fillable), and via electronic and web form submissions. 2. Health Imaging artifacts generated by medical systems such as, but not limited to, MRI devices, Ultrasound devices, X-Ray machines, laboratory applications as well as any medical device or application that collects patient data in the delivery of healthcare.3. Information is also collected from a variety of other IT systems and resources internal to the VAe VA. These data collections may be done using secure web portals and VPN connection as well as facility identified resources.

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.

Information obtained directly from the individual will be assumed to be accurate. Furthermore, individuals have the right to obtain access to their records and request correction to

them when necessary (see Section 7 for additional information). Patient demographic as well as income verification matching completed by automated tools with connections to the Austin Automation Center are obtained. Practitioner's review and sign all treatment information and Business Office/Health Information Management Service reviews data obtained and assists with corrections.. The Federal Bureau of Investigation and Office of Personnel Management are contacted to obtain background reviews. Provider credentialing information is obtained from a variety of education resources. Data is correlated to patient records by key record identifiers. As stated previously, the data is reviewed for accuracy by the practitioner inputting the data prior to commitment to the system.

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?

The system does not check for accuracy by accessing a commercial aggregator of information.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

The 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 Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the: Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules). 24VA10A7 Patient Medical Records – VA 2020-21426.pdf (govinfo.gov)79VA10/85 FR 84114 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 National Vista Imaging System contains sensitive personal information – including social security numbers, names, and protected health information – on Veterans, members and Dependents This data is collected, stored and delivered to conduct the primary business of the Veterans Health Administration (VHA) which is to deliver top notch healthcare to our nation's Veterans. All the data collected is directly relevant to that mission as it ensures VA clinicians have access to the full Veteran healthcare picture when making critical decisions regarding the delivery and management of that healthcare. All data is collected and stored with the knowledge and authorization of the individual for whom the data references, i.e the patient or VA administrative staff. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm, embarrassment or even identity theft may result.

All data collected from DoD is directly relevant to the shared mission outlined in Presidential Review Directive #5, August 1998 to address the health preparedness and readjustment of Veterans and their families after deployments as well as the need to improve cooperation and coordination between DoD, VA, and HHS, such as the sharing of health information, to maintain the health of military personnel, Veterans, and their families.

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 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.

PII/PHI Data Element	Internal Use	External Use
Name	Used to identify the patient during appointments and in other forms of communication	Not used
Social Security Number	Used as a patient identifier and as a resource for verifying income Information with the Social Security Administration	Not used
Date of Birth	Used to identify age and confirm patient identity	Not used
Maiden Name	Used to confirm patient identity	Not used
Mailing Address	Used for communication, billing purposes and calculate travel pay	Not used
Zip Code	Used for communication, billing purposes, and to calculate travel pay	Not used
Phone Number(s)	Used for communication, confirmation of appointments and conduct Telehealth appointments	Not used
Fax Number	Used to send forms of communication and records to business contacts, Insurance companies and health care providers	Not used

Email Address	Used for communication and MyHealtheVet secure communications	Not used
Emergency Contact Information (Name, Phone Number, etc. of a different individual)	Used in cases of emergent situations such as medical emergencies	Not used
Financial Account Information	Used to calculate co-payments and VA health care benefit eligibility	Not used
Health Insurance Beneficiary Account Numbers	Used to communicate and bill third part Health care plans	Not used
Certificate/License numbers	Used to track and verify legal authority to practice medicine and Licensure for health care workers in an area of expertise	Not used
Current Medications	Used within the medical records for health care purposes/treatment, prescribing medications and allergy interactions	Not used
Previous Medical Records	Used for continuity of health care	Not used
Race/Ethnicity	Used for patient demographic information and for indicators of ethnicity-related diseases	Not used
Radiology Number (RAD)	Used to track images	Not used
Consult Number (CON)	Used to track patient consultations	Not used
Study Number	Used to track studies	Not used
X-ray Technician Name	Used to identify image origin	Not used
Facility Name	Used to identify location of service	Not used
Reason for Image	Used to identify reason for image	Not used
What Type of Study	Used to identify type of study	Not used
Clinical images	Used to track patient images	Not used
Scanned documents	Used to track documents submitted	Not used
Motion video, and other non-textual data files.	Used for patient care	Not used
Patient data	Used for patient care	Not used

Patient data locations	Used to identify where patients are care for	Not used
DICOM images	Used for patient care	Not used
Benefits	Used to identify patient eligibility	Not used
Clinical images	Used for patient care	Not used
Claims Decision	Used to identify status of claim	Not used
DD-214	Used to determine patient eligibility	Not used
System Log files	Used to troubleshoot system errors	Not used
Cache log	Used to troubleshoot system errors	Not used
Text files	Used to troubleshoot system errors	Not used

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?

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

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

The system does not create or make available new or previously unutilized information about an individual.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?
Data at rest is encrypted by way of IAAMS, It uses the follow: CTERA: DHE, ECDHE and RSA (with AES-256), Cisco HX: ECDHE.

Data in transit via the Wide area network is encrypted by way of the network routers. Data in transit via Local area network does not currently encrypt data in all instances. VistA Imaging Development team is currently working to remediate this issue with an estimated resolution date of 1 April 2025.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
SSNs are stored in globals in VistA, which are protected by Options and Keys. HDIG log files containing SSN info are encrypted Images are stored on storage servers and locked against unauthorized access via Share and NTFS permissions

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

Data in transit via the Wide are network is encrypted by the Network routers and due to the design and configuration of this FDA approved device, data at rest is encrypted.

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

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

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

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

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

2.4a How is access to the PII determined?

Access to the Vista Imaging system 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 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. Please reference the individuals Privacy Impact Assessments for each facility to learn more. http://www.privacy.va.gov/privacy_impact_assessment.aspAdditionally, 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. DoD clinicians access the clinical imaging documentation provided via VistA Imaging through secure DoD electronic health record systems including Armed Forces Health Longitudinal Technology Application (AHLTA), Joint Legacy Viewer (JLV) and Health Artifact and Image Management Solution (HAIMS). Specific security requirements for communications between DoD and VA are documented in the MEDCOI Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) between the Defense Health Agency (DHA) and VA. These requirements include provisions for access control, auditing, authentication, configuration, contingency planning, disaster recovery, incident response, monitoring, and training.

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

Each facility defines criteria, procedures, controls, and responsibilities regarding access

2.4c Does access require manager approval?

Yes

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

Yes

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

All personnel with access to VistA Imaging

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Zip Code, Phone Number(s), Fax Number, Email Address, Emergency Contact Information (Name, Phone Number, etc. of a different individual), Financial Account Information, Health Insurance Beneficiary Account Numbers, Certificate/License numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Radiology Number (RAD), Consult Number (CON) , Study Number , X-ray Technician Name , Facility Name , Reason for Image , What Type of Study, Clinical images, Scanned documents, Motion video, and other non-textual data files. , Patient data, Patient data locations, DICOM images, Benefits, Clinical images, Scanned documents, Motion video, Other non-textual data files, Claims Decision, DD-214, System Log files, Cache log, Text files.

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.*

When managing and maintaining VA data and records, all healthcare facilities will follow the guidelines established in VA Record Control Schedule (RCS)10-1 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf).This document specifies how long records will be retained by the VA, if/when they will be transferred to a national records storage location, and the length of time the records will be stored at the national level. For greater details related to records retention at the Veterans' Health Administration, please review RCS-10-1. Below are some key record retention schedules for your information: Health Records Folder File or CHR (Consolidated Health Record) contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. Once designated an inactive medical record, it will be moved to a VA records storage facility. Patient medical records are retained for a total of 75

years after the last episode of care. (Department of Veterans Affairs Record Control Schedule (RCS)10-1 , Chapter Six- Healthcare Records, Item 6000.1 and 6000.2.Health Record Folders and Electronic Health records. 79VA10 states RCS 10–1, Item 2000.2 Information Technology Operations and Maintenance Records destroy 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use (DAA–GRS–2013–0005– 0004, item 020). RCS10–1, Item 2100.3 2100.3, System Access Records destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use (DAA–GRS–2013–0006– 0004, item 31). https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

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?

When managing, and maintaining VA data and records, All healthcare facilities will follow the guidelines established in the VA and NARA-approved Department of Veterans' Affairs Record Control Schedule (RCS)10-1 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf).

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

When managing, and maintaining VA data and records, All healthcare facilities will follow the guidelines established in the VA and NARA-approved Department of Veterans' Affairs Record Control Schedule (RCS)10-1 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf).

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

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

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.

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

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: In complying with VA and NARA retention mandates, in many cases the data stored in Vista Imaging will outlive those it is intended to benefit. It is easy to anticipate an increased risk to patient privacy as technology advances and the balance between malicious intrusion/prevention is continuously tested.

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

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VistA Image Exchange (CVIX/VIX)	Patient care	Clinical images, scanned documents, motion video, and other non-textual data files. Patient data, Patient data locations	DICOM, FHIR metadata
VistA (for the CVIX/VIX)	Patient care	Patient Information, Patient Data, Patient Data locations	RPC, HTTPS
Image Viewer	Patient care	Clinical images, scanned documents, motion video, and other non-textual data files. Patient data, Patient data locations	RPC
Image Capture	Patient care	Clinical images, scanned documents, motion video, and other non-textual data files. Patient data, Patient data locations	RPC
ISI RAD	Patient care	Clinical images, motion video, and other non-textual data files. Patient data, Patient data locations	RPC
DICOM Importer	Patient care	DICOM images	HTTP/HTTPS
HDIG	Patient care	Clinical images	RPC, DICOM
Station 200 (STA200)	Patient care	Patient Information, Patient data, Patient data locations	RPC, HTTPS
PACS	Patient care	Patient Information. Patient Data listings. Patient data locations	HL7 & DICOM
Joint Legacy Viewer (JLV)	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,	HTTP/HTTPS

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*
		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, 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	
Joint Legacy Viewer-Community Viewer	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, Other Unique Identifying Information (list below); Radiology Number (RAD), Consult Number (CON), Study Number, X-ray	HTTP/HTTPS

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*
		Technician Name, Facility Name, Reason for Image, What Type of Study	
MyHealtheVet	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, 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	HTTP/HTTPS
Image Viewing Solution (IVS-Mobile Apps)	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	HTTP/HTTPS

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*
		Numbers Account numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, 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	
Embedded Fragment Registry (EFR)	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, 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	RPC, HTTP/HTTPS
RefDoc	Patient care	Name, Social Security Number, Date of Birth,	RPC, HTTP/HTTPS

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*
		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, 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	
After Visit Summary (AWS)	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, Other	RPC, HTTP/HTTPS

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*
		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	
EHRM TeleReader Service	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, 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	RPC, HTTP/HTTPS
IaaMS	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,	RPC, HTTP/HTTPS

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*
		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, 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	
DSS Enterprise (DocManager VistA Scanning & Indexing System)	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, Other Unique Identifying Information (list below); Radiology Number (RAD), Consult Number (CON), Study Number, X-ray	RPC, HTTP/HTTPS

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*
		Technician Name, Facility Name, Reason for Image, What Type of Study	
Veterans Benefits Management System (VBMS)	Patient care	Social Security Number, Benefits Information, Claims Decision, DD-214	Compensation and Pension Record Interchange (CAPRI) electronic software pack
Vista	Patient care	System Log files, sample clinical data that may contain Protected Health Information (PHI)	Electronically pulled from VistA thru Computerized Patient Record System (CPR
VistA Imaging	Patient care	Social Security Number, Benefits Information, Claims Decision, DD-214	Compensation and Pension Record Interchange (CAPRI) electronic software pack
Vista	Patient care	System Log files, cache log files, images, text files, clinical data, etc., all contain PII/PHI	RPC Calls or web services over HTTPS using TLS version 1.2 encryption.
VistA Imaging	Patient care	System Log files, cache log files, images, text files, clinical data, etc., all contain PII/PHI	RPC Calls or web services over HTTPS using TLS version 1.2 encryption.
VistA	Patient care	Patient Information, Patient data, Patient data locations	RPC, HTTPS
Station 200 (STA200)	Patient care	Patient Information, Patient data, Patient data locations	RPC, HTTPS

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*
SCIP VAEC	Patient care	Clinical images, Patient data	DICOM, FHIR meta
Community Image Exchange Service (CIES)	Patient care	Clinical images, scanned documents, motion video, and other non-textual data files. Patient data, Patient data locations	HTTPS, DICOM

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The sharing of data is necessary for the medical care of individuals eligible to receive care at VHA and individual facilities. 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				

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: State there is no external sharing

Mitigation: State there is no external sharing

Section 6. Notice

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

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

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

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

The VHA Notice of Privacy Practice (NOPP) https://dvagov.sharepoint.com/sites/VHAABQIntranet/Org/Dir/DirDocs/Forms/AllItems.aspx?id=%2Fsites%2FVHAABQIntranet%2FOrg%2FDir%2FDirDocs%2FNOPP%2Epdf&parent=%2Fsites%2FVHAABQIntranet%2FOrg%2FDir%2FDirDocs 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. 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):1) The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN24VA10A7, 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. 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. 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."

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

https://www.va.gov/files/2022-10/NOPP%20IB_163p%20Final%209-30-2022%20508%20Compliant.pdf

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. The VHA Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter.

This Privacy Impact Assessment (PIA) also serves as notice 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."

A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority and the conditions under which the information can be disclosed.

Notice is also provided in the SORN Patient Medical Records-VA, SORN24VA10A7, 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. 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.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.

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.

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.

Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.
Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent.
Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written 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, information is not disclosed from the facility directory unless otherwise required by law.

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

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

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

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

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. 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?

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.***
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.In addition to the procedures discussed above, the SORNs listed in the Overview section of this PIA each address record access, redress, and correction. Links to all VA SORNs can be found at https://www.oprm.va.gov/docs/Current_SORN_List_10_19_2021.pdf. Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact Contract Officer Representative to obtain information upon request.

7.1b If the system is exempt, 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)?

System is not exempt from the access provisions of the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

System is a Privacy Act system.

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 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.

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. ***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. In addition to the formal procedures discussed in question 7.2 to request changes to one's health record, a Veteran or other VAMC patient who is enrolled in MyHealtheVet can use the system to make direct edits to their health records.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that 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?

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?
Access to each VI facility working and storage areas is restricted to VA employees who must complete both the HIPAA 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.

8.1b 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?

Users from outside agencies is unauthorized.

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

Roles within the system are determined by menu and key settings. Roles are assigned by position and approved by the supervisors who the assign/approve the menus and keys settings.

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 HIPAA 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.

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 privacy HIPAA training. Finally, all new employees receive face-to-face training by the facility Privacy Officer and Information Security Officer during new employee orientation.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* June 2, 2023
3. *The Authorization Status:* Authorization to Operate
4. *The Authorization Date:* Jul 24, 2023
5. *The Authorization Termination Date:* Jul 23, 2025
6. *The Risk Review Completion Date:* Jun 2, 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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

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

Section 9 – Technology Usage

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

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?
If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.
Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

VistA Imaging utilizes VA Enterprise Cloud (VAEC) 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). (*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.

System does not have a contract Cloud service provider.

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.

System does not collect any ancillary data.

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

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

System does not have any contracts with cloud providers.

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).

System does not utilize RPA.

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

ID	Privacy Controls
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.

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2024.07.26 08:54:45 -04'00'

Privacy Officer, Nancy Katz-Johnson

TRISTAN CARROLL

Digitally signed by TRISTAN CARROLL
Date: 2024.08.01 09:48:51 -05'00'

Information System Security Officer, Tristan Carroll

LARRY BROWN

Digitally signed by LARRY BROWN
Date: 2024.08.01 13:30:35 -04'00'

Information System Owner, Larry Brown

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

https://www.va.gov/files/2022-10/NOPP%20IB_163p%20Final%209-30-2022%20508%20Compliant.pdf

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 1605.04