Privacy Impact Assessment for the VA IT System called:

VISN 23 Visage PACS

Veterans Health Administration

VISN 23 HTM/Imaging Service Line

eMASS ID 2507

Date PIA submitted for review:

July 23, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Karyn Volkmann	Karyn.Volkmann@va.gov	402-995-3427
Information System Security Officer (ISSO)	Stuart Chase	Stuart.chase@va.gov	410-340-2018
Information System Owner	Jeremy Achterhoff	Jeremy.achterhoff@va.gov	402-218-3050

Abstract

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

VISN 23 Visage PACS is the replacement Picture Archive and Communication System (PACS) for VISN 23 Radiology/HTM. This system will enable image review and interpretation of diagnostic images across VA-VISN 23 facilities. VISN 23 Visage PACS is replacing the current "on prem" Visage system and Acuo VNA hosted in all 8 VISN 23 facility data centers. VISN 23 Visage PACS, VASI ID # 2845, is a comprehensive Radiology image management and reporting system that will allow VISN 23 Radiologists to more efficiently and more effectively interpret and report imaging studies. The VISN 23 Visage PACS is comprised of an image archive, Radiologist worklist, and image viewing suite. This PACS system is designated as a medical system with FDA 510K approval.

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?

VISN 23 Visage PACS (Picture Archive and Communication System)- VISN 23 Radiology/VISN 23 HTM.

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

VISN 23 Visage PACS provides the capability for radiology-based image review and interpretation across VISN 23 by Radiologists.

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

VISN 23 HTM is responsible for the procurement funding, deployment, management, and sustainment of the VISN 23 Visage PACS.

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?

VISN 23 Visage PACS is an VISN 23 medical system that stores diagnostic radiology images (CTs, MRIs, Ultrasounds, and Digital X-rays) for every patient whose images are acquired by VISN 23. Our current PACS solution houses approximately 5.5 million studies and keeps 10 years' worth of studies, anything older is archived in VistA Imaging.

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

Information includes both diagnostic images as referenced above and their associated interpretations/reports. The images and associated reports are utilized by VHA referring physicians for the diagnosis, treatment, and clinical management of patients.

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

VISN 23 Visage PACS interfaces with National Teleradiology Program (NTP) for teleradiology remote reads after hours and on weekends when VISN 23 medical centers do not have local Radiologist coverage. VISN 23 Visage PACS will also interface with Corepoint Integration Engine for HL7 communication to VistA, as well as VHA Compass Routers for DICOM transfer to VistA Imaging.

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?

VISN 23 Visage PACS is an VISN PACS that is maintained/managed centrally by VISN 23 HTM with a pending ATO for VA Enterprise Cloud deployment. Standard role-based security will be deployed in the system with least privileges model.

3. Legal Authority and SORN

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

SORN 79VA10 "Veterans Health Information Systems and Technology Architecture (VistA) Records -VA" which has authority to maintain the records under Title 38, United States Code, Section 501(b) and 304.
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?

No SORN amendment or revision will be required for this system

4. System Changes

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

Business processes will remain in place with this replacement PACS. We are migrating from an on-prem based system that is EOL to a VAEC based system with the same overall clinical function.

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

Existing EOL system is being replaced with a state-of-the-art radiology PACS that is cloud-based.

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
- ☐ (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Other PII/PHI data elements: Patient ID, Patient Height/weight, Patient age, Lab data tied to some HL7 messages

Note Medical Records to include medical history, reason for exam, relevant clinical information and previous radiology reports.

PII Mapping of Components (Servers/Database)

VISN23 Visage PACS consists of 1 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 VISN23 Visage PACS and the reasons for the collection of the PII are in the table below.

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

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.

Internal Components Table

Component Name (Database, Instances,Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

Visage PACS database	Yes	Yes	• Name
			• SSN
			• Patient Date of Birth
			• Personal Mailing Address
			• Personal Phone Number(s)
			• Medical Records to include medical history, reason for exam, relevant clinical information, and previous radiology reports.
			• Race/Ethnicity
			• Medical Record Number (MRN) (could be patient ID)
			• Gender
			• Other Data Elements
			  ○ Patient ID
			  ○ Patient Height/weight
			  ○ Patient Age
			  ○ Lab data tied to some HL7 messages
				Patient identification, study reconciliation, and patient diagnosis	Data is encrypted at rest and in transit and only the VHA clinical staff and technical staff with a right to know can access the system.

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?

Images are received from facility imaging modalities and Radiology order/report information is received via HL7 interfaces from the VHA's medical records.

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 is transmitted from the imaging modalities and medical record to VISN 23 Visage PACS. We only receive data from VHA systems used in the treatment and care of the patients.

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

A radiology report is generated by VISN 23 Physicians using the VISN 23 PACS and that report is transmitted back to the EMR via Corepoint as the HL7 interface.

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?

DICOM images are transmitted electronically between the facility imaging modalities and the VISN 23 PACS and HL7 messages are transmitted electronically between the EMR (VistA) and Corepoint and then to the VISN 23 PACS.

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?

The information is not collected on a form and is not subject to the Paperwork Reduction Act.

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 used by the system is from an individual's medical record and is checked for accuracy by medical staff at and during the point of care. VISN 23 Radiology has a QA process in place for identifying and responding to potential inaccuracies in data where there are identified discrepancies between patient demographic data and the acquired images.

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 using a commercial aggregator of information. However, the VISN 23 Visage PACS system does receive its HL7 feed from Corepoint, which will normalize the HL7 data prior to sending into NTP NextGen PACS. Both Corepoint and VISN 23 Visage PACS will validate message content and structure to ensure that it meets pre-defined standards according to the Interface Control Document (ICD) and established HL7 standards.

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 information collected by this system is obtained from SORNs 79VA10 Veterans Health Information Systems and Technology Architecture (VistA) Records - VA and 24VA10A7 "Patient Medical Record-VA" which has the authority to maintain the records under Title 38, United States Code, Section 501(b) and 304.

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

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

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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: Due to the highly sensitive nature of the data collected, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, it could result in professional, or other harm to the Veterans impacted.

Mitigation: Access controls are in place to limit access to those VA employees who have a need to know for their official job duties. The VISN 23 Visage PACS system will be isolated per Medical Device Isolation Architecture (MDIA) guidance and will not have access to the Internet.

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	Identify the Patient	Not used
Social Security Number (SSN)	Identify the Patient	Not used
Date of Birth (DOB)	Identify the Patient	Not used
Personal Mailing Address	Not used within VISN 23 Visage PACS but required data element for VistA HL7 2.4	Not used
Personal Phone Number(s)	Not used within VISN 23 Visage PACS but required data element for VistA HL7 2.4	Not used
Medical Records to include medical history, reason for exam, relevant clinical information, and previous radiology reports	Medical history, reason for exam, relevant clinical information and previous radiology exams and reports are used by the interpreting Radiologists to inform their diagnosis.	Not used
Race/ethnicity	Identify the Patient	Not Used
MRN	Identify the Patient	Not used
Gender	Identify the Patient	Not used
Other Data Elements • Patient ID • Patient Height/weight	Not used within VISN 23 Visage PACS but required data element for VistA HL7 2.4	Not used

• Patient Age • Lab data tied to some HL7 messages		

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?

VISN 23 Visage PACS utilizes state-of-the-art artificial intelligence (AI) for the detection of intracranial hemorrhage (ICH) and flags suspected stroke cases for Physician review with computed tomography (CT) DICOM images. The VISN 23 Visage PACS has other analytics tools in place to identify and escalate the priority of various radiology studies, such as stroke exams and intraoperative radiographs.

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 VISN 23 Radiologists will dictate a radiology report based on the DICOM images and HL7 clinical information received. This radiology report will be transmitted via HL7 to the EMR (VistA). The radiology report will then be accessible in the patient chart and other Physicians will act on this clinical information and adjust the treatment and care of Patients.

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?

The system will be deployed in VA Enterprise Cloud (FISMA High) with encrypted data at rest. Data in transit will be encrypted across the VA WAN.

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

The system will be isolated behind a firewall per MDIA guidance. Physical access to the system will be restricted to system administrators and approved by the Business Owner via ePAS portal. The

system will be secured with Microsoft Defender for antivirus. The system will be hosted in VA Enterprise Cloud (FISMA High) and the data will be encrypted in transit and at rest.

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

System administrators and clinical end-users go through annual VA Privacy and Information Security training. The system will be isolated per MDIA guidance and will be hosted in VA Enterprise Cloud. Data in transit and at rest will be encrypted. Administrative access to the servers will be restricted to system administrators. The system will use role-based access to sensitive information.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to PII will be done using role-based least privilege access. PII will be accessed by clinical users, such as VISN 23 Radiologists, in the performance of their clinical duties within the scope of their privileges.

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

Administrative access to the system is limited to system administrators and is approved and documented by the Business Owner through ePAS portal. End-user access is role-based and is approved by the VISN 23 Clinical Supervisor and VISN 23 System Administrators and is overseen by the Business Owner. Access logs are maintained with the VISN 23 Visage PACS system in compliance with HIPAA requirements.

2.4c Does access require manager approval?

Access to the VISN 23 Visage PACS will be allocated by role with approval by the VISN 23 Clinical Supervisor and VISN 23 System Administrators designating the necessary role and access needed per user.

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

Access to PII is monitored and recorded and can be tracked as needed in compliance with HIPAA requirements. This will be done through audit logs in the VISN 23 Visage PACS application.

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

Business Owner and NTP System Administrators.

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*

All information collected from question 1.1 is retained by the system for clinical care along with the diagnostic images.

3.2 How long is information retained?

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

The official archive/patient record is the EMR. Final radiology reports are transmitted back to the EMR for retention. On the VISN 23 Visage PACS, the system will include a long-term image archive with reports/images retained for the life of the system, but ultimately the EMR is the long term repository of the Radiology reports.

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?

The records for this system are maintained under the VA Records Control Schedule (RCS 10-1) 6000.2.c(1) with disposition authority N1-15-02-3, item 4 which permits the record to be destroyed when it is no longer needed for administrative or clinical operations.
https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf.

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

The records for this system are maintained under the VA Records Control Schedule (RCS 10-1) 6000.2.c(1) with disposition authority N1-15-02-3, item 4.
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.

There are no paper records. Electronic records will be purged with the hard drives and/or virtual machine (VM) instances destroyed at the end of the contract with the VISN 23 Visage PACS vendor.

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 system will utilize a test environment for testing/development and test patients will be used in this environment. The VISN 23 Visage PACS will not be used for research. Clinical end-users will be trained on the use of the application and will have access to anonymized test studies (i.e., teaching files).

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: There is a risk that the information maintained by the system could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released, breached, or exploited for reasons other than what is described in the privacy documentation associated with the information.

Mitigation: To mitigate the risk posed by information retention, the system will adhere to the VA RCS schedules for each category or data it maintains. When the retention date is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***

VA ATO Boundaries
 	
• NTP NextGen PACS
• VistA
• VistA Imaging
	VISN 23 VISAGE stores patient information in VistA and VistA Imaging per VA Policy. VistA Imaging is the system of record for imaging for the VA. VistA is the system of record for the electronic medical record.
	
	NTP NextGen PACS is a service within the VA used for after hours Radiologist coverage when sites do not have a Radiologist on site to read/interpret
		• Name
		• SSN
		• Patient Date of Birth
		• Personal Mailing Address
		• Personal Phone Number(s)
		• Medical Records to include medical history, reason for exam, relevant clinical information, and previous radiology reports.
		• Race/Ethnicity
		• Medical Record Number (MRN) (could be patient ID)
		• Gender
		• Other Data Elements
		  ○ Patient ID
		  ○ Patient Height/weight
		  ○ Patient Age
		  ○ Lab data tied to some HL7 messages
			Electronic submission of HL7 messages specific to radiology; all radiology HL7 Observation result (ORU) and Order Message (ORM) are transmitted over TCP/IP.

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*

VHA Interfaces
• Medicalis
• Corepoint
• Compass
	VHA Interfaces are used as a passthrough of data to the VHA ATO boundaries listed above.
	
	Medicalis handles workflows for VHA Radiologists.
	
	Corepoint handles HL7 traffic from VISN23 VISAGE to VistA.
	
	Compass handles all Diacom (Image) routing.
		• Name
		• SSN
		• Patient Date of Birth
		• Personal Mailing Address
		• Personal Phone Number(s)
		• Medical Records to include medical history, reason for exam, relevant clinical information, and previous radiology reports.
		• Race/Ethnicity
		• Medical Record Number (MRN) (could be patient ID)
		• Gender
		• Other Data Elements
		  ○ Patient ID
		  ○ Patient Height/weight
		  ○ Patient Age
		  ○ Lab data tied to some HL7 messages
			HL7 and DICOM over Network TCP/IP

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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:

<u>Privacy Risk:</u> There is a risk that information may be shared with unauthorized VA program or system or that data could be shared.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of two factor authentication for access to the application, data encryption at rest and in transit, and role-based access authorization are all measures that are utilized.

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***	***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***	***List the method of transmission and the measures in place to secure data***

	office or IT system		***sharing (can be more than one)***	
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: No external sharing.

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

Notice is also provided in the Federal Register with the publication of the SORN 79VA10 "Veterans Health Information Systems and Technology Architecture (VistA) Records-VA ", https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf . 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."

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

Notice was provided as stated in 6.1a.

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.

Notice was provided as stated in 6.1a.

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.

Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them.

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.

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 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: There is a risk that veterans and other members of the public will not know that the system exists or that it collects, maintains, and/or disseminates PII, PHI or PII/PHI about them.

Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans are enrolled for health care. 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 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.***

There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office. VHA Directive 1605.01, Privacy and Release of Information, outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access.VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

The system is not exempt.

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?

This system falls under the following SORNs.
79VA10 Veterans Health Information Systems and Technology Architecture (VistA) Records - VA and 24VA10A7 "Patient Medical Record-VA"
The information is collected from the Veteran medical record, and it may be obtained as described in section 7.1a above.

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.

While there are no processes for amending information that is in this system, the information is obtained from the Veteran Medical record which can be amended. The VHA Notice of Privacy Practices informs individuals how to file an amendment request with VHA. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to

be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. That is, VA must maintain in its records only such information about an individual that is accurate, complete, timely, relevant, and necessary. Individuals have the right to review and change their contact or demographic information at time of appointment or upon arrival to the VA facility and/or submit a change of address request form to the facility business office for processing. If corrections are needed for legal name, date of birth, or Social Security Number (SSN) changes, Patient Registration would process the request requiring a valid driver's license, state identification, passport, military ID, or a letter from the Social Security Administration stating the changes and a wet signature from the individual requesting the change. The facility Privacy Officer reviews and approves these changes as well.

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 VHA 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 Individuals seeking information regarding access to and contesting of VA benefits records may write, call or visit the nearest VA regional office.

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

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.

Formal redress via the amendment process is available to all individuals, as stated in questions 7.1-7.3. Redress is provided through the Privacy Act for the individual to view and request correction to

the inaccurate or erroneous information. If the request is denied, the individual to appeal the decision by writing to the Office of General Counsel (024); Department of Veterans Affairs; 810 Vermont Avenue, N.W.; Washington, D.C. 20420. The Privacy Act and HIPAA permit the individual to also complete a Statement of Disagreement to the information that was denied correction. The facility would be able to include a rebuttal to the Statement of Disagreement. The Statement of Disagreement, rebuttal, and denial letter would be attached to the information that was requested to be corrected and would be released with the information at any time the information was authorized for release. Veterans can also update their personal information through My HealtheVet (MHV). Information they can update includes things such as demographics and secure messaging.

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 members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: The system 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. As discussed in question 7.3, the NOPP, which every enrolled Veteran receives every three years or when there is a major change. The NOPP discusses the process for requesting an amendment to one's records. The VISN 4 facilities Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information. The Veterans' Health Administration (VHA) established MyHealthyVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account 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?

Individuals that require access to the VISN 23 Visage PACS system, such as radiologists, PACS administrators, and support staff/radiology technologist will be granted role-based access. This limits the level of access based on roles. This will be determined by supervisors and/or radiology section chiefs.

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?

The only users from other agencies that will require access to the system are for vendor remote support. Individuals will be credentialed and go through a background investigation prior to being permitted access to the VISN 23 Visage PACS system. PII will not be shared.

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

There are several different roles within the application. These are the basic functions that each group has been granted access to do within the NTP NextGen PACS application.
Radiologist – view and/or fetch registered radiology studies, dictate and/or addend radiology reports, communicate with other radiologists and technologists, view and/or create clinical notes.
Technologist – view and/or fetch registered radiology studies, view DICOM information, view and/or fetch registered radiology studies, communicate with radiologists, view DICOM monitoring queues, perform study reconciliation and quality control, view and/or create clinical notes
Clinician – view and/or fetch registered radiology studies, view clinical notes
PACS Administrators – create/modify DICOM nodes, add new users, view and/or fetch registered radiology studies, communicate with radiologists and technologists, view and/or create clinical notes, view DICOM monitoring queues, perform study reconciliation and quality control, view and track audit logs.

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.
VA contractors from Visage Imaging will have access to the system and to PII within the system. A BAA is in place and each contractor that will have access to the system will undergo a background investigation and be required to annually complete VA Talent Management System (TMS) Privacy and Security training for system administrators.

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.

Annual VA Talent Management System (TMS) Privacy and Security training is required for system administrators and end-users that will access the system.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* <<ADD ANSWER HERE>>
2. *The System Security Plan Status Date:* <<ADD ANSWER HERE>>
3. *The Authorization Status:* <<ADD ANSWER HERE>>
4. *The Authorization Date:* <<ADD ANSWER HERE>>
5. *The Authorization Termination Date:* <<ADD ANSWER HERE>>
6. *The Risk Review Completion Date:* <<ADD ANSWER HERE>>
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* <<ADD ANSWER HERE>>

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.***

System is pursuing ATO – IOC Date expected 01/01/2025

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used

for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.
Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

The VISN 23 Visage PACS will be deployed in VA Enterprise Cloud – AWS GOV Cloud. AWS GOV Cloud has FedRAMP High Authorization. The cloud model that will be utilized is Platform as a Service (PaaS) wherever possible, otherwise Infrastructure as a Service (IaaS).

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.*

Contract # 36C26324Q0167

Information made available to the contractor or subcontractor by VA for the performance or administration of this contract or information developed by the contractor/subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the contractor/subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

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.

Per AWS, they do not collect any ancillary data and thererefore, could not be compromised and used in subsequent attacks as it doesn't exist.

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.

A Privacy Service with Office of Acquisition and Logistics (OAL) and Office of Operations, Security, and Preparedness (OSP) establish privacy roles, responsibilities, and access requirements for contractors in the Organizational Rules of Behavior (ROB), VA Directive 6500 (page 9 of 39) and in the APPENDIX C of VA Handbook 6500.6 to be included in

contracts. Contractors take privacy training and sign the Rules of Behavior (ROB) before gaining access to VA networks and information in support of contracts

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).

No

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

KARYN VOLKMANN

Digitally signed by KARYN VOLKMANN
Date: 2024.08.19 13:58:39 -05'00'

Privacy Officer, Karyn Volkmann

STUART CHASE

Digitally signed by STUART CHASE
Date: 2024.08.19 15:23:40 -04'00'

Information System Security Officer, Stuart Chase

JEREMY ACHTERHOFF

Digitally signed by JEREMY ACHTERHOFF
Date: 2024.08.16 07:31:56 -05'00'

Information System Owner, Jeremy Achterhoff

APPENDIX A-6.1

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
explains the collection and use of protected health information to individuals receiving health care from VA.

Notice is also provided in the Federal Register with the publication of the SORN 79VA10 “Veterans Health Information Systems and Technology Architecture (VistA) Records-VA “, https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf . 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.”

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