



Privacy Impact Assessment for the VA IT System called:

VISN 19 AGFA PACS VNA (VAEC)

Veterans Health Administration

VISN 19 Healthcare Technology Management

eMASS ID #: 2317

Date PIA submitted for review:

5/8/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	John McKinney	John.mckinney@va.gov	970-836-4284
Information System Security Officer (ISSO)	Eduardo Lorenzo	Eduardo.lorenzo@va.gov	303-808-7703
Information System Owner	Kelly Luu	Kelly.luu@va.gov	720-441-7999

Abstract

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

VISN 19 AGFA PACS VNA (VAEC) is a COTS application used to archive and retrieve radiology images. The application interfaces with commercial PACS for storage and retrieval of high resolution imagery. The system intelligently assesses future workload to transfer clinical images from the archive to the on-prem PACS system prior to patient visits to improve image load latency when clinicians are reviewing historical imagery. AGFA PACS VNA is a cloud hosted vendor neutral archive. The environment includes a development and production environment (two availability zones). Within this environment virtual servers reside running Oracle Linux 8 for application, database, and load balancing servers. Windows server 2019 is also deployed for the Core application server. The system makes VA connections back to AGFA PACS servers in VISN 19, active directory, and has a VISTA HL7 connection.

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 19 AGFA PACS VNA (VAEC) is owned by VISN 19 Healthcare Technology Management.

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

This IT system allows for the long-term storage of DICOM images from any PACS or imaging modality vendor. The system maintains full quality images, manages the distribution of patient prior images to facility PACS systems and provides a web-based image viewer for users without access to the full on-premises PACS system. This system helps fulfill the agency mission of caring for veterans by improving care in the Radiology, Cardiology, and Oncology spaces. By providing on time and accurate prior images to doctors, proper assessments can be made about temporal improvement or deterioration of medical conditions.

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

VA Owned and VA Operated

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 19 Estimates that up to 1,000,000 individuals may have information stored in the system. The typical client is a United State Military Veterans whose care at VA within VISN 19 requires imaging in the Radiology Department.

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

Information stored in the system includes images collected by Radiology and Non-Radiology Imaging and Modalities and Patient Demographics

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

Information is shared for the purpose of healthcare operations between the system and other VA medical systems. PHI and PII is shared between V19VNA and Medical Information Systems (COTS PACS) within the MD-LITE boundary for diagnosis, treatment planning, and recovery assessment.

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?*

No, the VAEC deployment is the only AGFA VNA deployed in the enterprise.

3. *Legal Authority and SORN*

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Sections 501(b) and 304

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?*

System is not in the process of modification. SORN provides coverage for the cloud usage and storage.

4. *System Changes*

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

No

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

No

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:

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Health Insurance | <input type="checkbox"/> Integrated Control |
| <input checked="" type="checkbox"/> Social Security | <input type="checkbox"/> Beneficiary Numbers | <input type="checkbox"/> Number (ICN) |
| Number | <input type="checkbox"/> Account numbers | <input type="checkbox"/> Military |
| <input checked="" type="checkbox"/> Date of Birth | <input type="checkbox"/> Certificate/License | <input type="checkbox"/> History/Service |
| <input type="checkbox"/> Mother's Maiden Name | numbers ¹ | <input type="checkbox"/> Connection |
| <input checked="" type="checkbox"/> Personal Mailing | <input type="checkbox"/> Vehicle License Plate | <input type="checkbox"/> Next of Kin |
| Address | Number | <input checked="" type="checkbox"/> Other Data Elements |
| <input checked="" type="checkbox"/> Personal Phone | <input type="checkbox"/> Internet Protocol (IP) | (list below) |
| Number(s) | Address Numbers | |
| <input type="checkbox"/> Personal Fax Number | <input type="checkbox"/> Medications | |
| <input type="checkbox"/> Personal Email | <input checked="" type="checkbox"/> Medical Records | |
| Address | <input type="checkbox"/> Race/Ethnicity | |
| <input type="checkbox"/> Emergency Contact | <input type="checkbox"/> Tax Identification | |
| Information (Name, Phone | Number | |
| Number, etc. of a different | <input checked="" type="checkbox"/> Medical Record | |
| individual) | Number | |
| <input type="checkbox"/> Financial Information | <input checked="" type="checkbox"/> Gender | |

Other PII/PHI data elements: Marital Status, Radiological (X-Ray, Ultrasound, RF, CT, MRI, PET, SPECT, MAMMO) and Non-Radiological Images (Cardiac Ultrasound).

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

PII Mapping of Components (Servers/Database)

VISN 19 AGFA PACS VNA (VAEC) consists of 8 key components (servers/databases/instances/applications/software/application programming interfaces (API). Only one of these components processes and stores PII. The type of PII collected by VISN 19 AGFA PACS VNA (VAEC) 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.**

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
AGFA EI Database Server	Yes	Yes	<ul style="list-style-type: none"> • SSN • Name • Age • Sex • Date of Birth • Marital Status • Home Address • Phone Number • <i>Radiological (X-Ray, Ultrasound, RF, CT, MRI, PET, SPECT, MAMMO) and Non-Radiological Images (Cardiac Ultrasound)</i> 	PII is part of the metadata of the images sent to the vendor neutral archive and makes the data identifiable when searching for prior images of a patient with an upcoming imaging order.	Database is encrypted at rest

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?

Information is collected from the VA Medical Record (CPRS or Oracle Cerner) via HL7 feed. Medical Records (Radiology Images) are also sent to the system from the PACS systems in VISN 19 after being generated at the modality.

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.

Not Applicable.

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

No.

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?

Yes.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

Not Applicable, information is collected electronically or generated by computing resources other than this system.

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.

At system the Go-Live the accuracy of information is verified from receipt to storage to distribution. After Go-Live, information accuracy is checked monthly as part of normal system

checks. Information accuracy is also verified after major and minor updates. This is performed manually by support staff.

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?

No.

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

Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a)

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: Collection of the PII/ PHI in Table 1 is critical to the agencies mission in that it facilitates the quality of care provided to the veteran. Collection of PII/PHI allows for clinicians to have prior imagery at the right place at the right time to give historical context to disease progression, treatment efficacy, or injury recovery. In this manor, veterans receive timely and high quality care.

Principle of Minimization: Yes, all data collected is relevant to the caregiving nature of its collection. All data fields are necessary to ensure the correct veteran is identified for each relevant historical image to ensure a correct progression is provided to the caregiver and a fully informed diagnosis or prognosis is provided to patient.

Principle of Individual Participation: The system in question does not have a method to collect information from the individual as it has no interaction at the point of care. Rather, this system receives information from the system of record (VISTA) via an HL7 feed and that information is directly collected 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:

Due to the highly sensitive nature of shared data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

Mitigation:

VISN 19 AGFA PACS VNA employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include access control, awareness and training, audit and accountability, certification, accreditation, and security assessments, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, systems and services acquisition, system and communications protection, and system and information integrity. The AGFA PACS VNA employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives.

All employees and contractors with access to Veteran’s health information are required to complete the Privacy and HIPAA Focused training as well as the VA Privacy and Information Security Awareness & Rules of Behavior training annually. The VA enforces two-factor authentication by enforcing smartcard logon requirements. PIV cards are issued to employees, contractors, and partners in accordance with HSPD-12. The Personal Identity Verification (PIV) Program is an effort directed and managed by the Homeland Security Presidential Directive 12 (HSPD-12) Program Management Office (PMO). IT Operations and Services (ITOPS) Solution Delivery (SD) is responsible for the technical operations support of the PIV Card Management System. Information is not shared with other agencies without a Memorandum of Understanding (MOU) or other legal authority.

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	Patient Identification purposes	Not used
Home Address	Patient Identification purposes	Not used
Phone Number	Patient Identification purposes	Not used
Marital Status	Patient Identification purposes	Not used
Social Security Number	Patient Identification purposes	Not used
Birthday	Patient Identification purposes	Not used

Gender	Patient Identification purposes	Not used
Medical Record Number	Healthcare Operations	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?

This system performs no analysis. It is used to assess upcoming provider workloads and provide local PACS image caches with prior studies for clinician to have quick access to time history of images collected in the diagnosis and treatment of the patient.

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.

This system creates no new information.

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?

Both data in transit and data at rest are encrypted using industry standard practices. For data being transported to and from the health record and to and from the on premises PACS system SSL is employed. For data at rest, encryption provided by AWS S3 storage is employed. Full disk encryption is utilized for data at rest on servers.

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

This system does collect, process, retain social security numbers. Encryption methodologies listed in section 2.3a are employed to protect SSNs in various states throughout the system. Additionally, access to the system is privileged and managed by VA personnel responsible for the management and administration of the system. External access to the data is considered to be a zero-trust model. Only trusted connections with a valid BAA and MOU/ISA are permitted to access the system from a non-VA source.

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

PHI and PII at rest and in transport is encrypted, so that only those with authorized access are granted meaningful access to the PHI and PII. Administrative safeguards are in place to ensure access to systems is granted only to those with a need for patient care or healthcare operations. Using active directory, system access is auditable back to who has accessed records or systems.

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 and PHI provided to the client by the system is managed by VHA personnel at the request of VA clinical staff and at the discretion of the System Owner or their delegate. Access is permitted by inclusion in Windows security groups. Security group membership is verified every three months. Direct access to the system for administration and maintenance is managed by the system owner or their delegate through the VA EPAS system. Those accessing the system will be PIV employees or contractors with a successful background check. Those requesting direct system access to underlying infrastructure including AWS portal access or server access via RDP or SSH shall request their access through VA EPAS and utilize multifactor authentication via token or password vault to achieve access.

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

Yes

2.4c Does access require manager approval?

Yes

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

Yes, actions performed through VA's CyberArk MFA solution are recorded and stored.

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

The System Owner, Kelly Luu, and the System Steward, John Michael or their delegate as needed.

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 data listed in section 1.1 is retained by the system within its database. This includes: Name, Home Address, Phone Number, Social Security Number, Date of Birth, Marital Status, Medical Record Number, and Medical Records.

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 data is retained throughout the care period of the patient and 7 years beyond that period.

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?

In accordance with the SORN and the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6.

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

In accordance with the SORN and the records disposition authority approved by the

Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6.

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.

All data in this system is digital. At the end of the retention period data is purged from the database and digitally destroyed.

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.

PII and PHI used in the course of testing and training is false in nature. The records are used in these cases or made up (e.g. SSN is 123-45-6789 or name is Bruce Wayne). In other cases studies may be de-identified before being used in for training purposes. VHA VISN 19 HTM utilizes Laurel Bridge Compass Router for de-identification and anonymization of 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 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, AGFA PACS VNA adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the system will carefully dispose of the data by the determined method as described in question 3.4. The AGFA PACS VNA ensures that all personnel involved with the collection, use and retention of data are trained in the correct process for collecting, using and retaining this data. A Records Management Officer (RMO), Privacy Officer (PO) and an Information System Security Officer (ISSO) are assigned to ensure their respective programs are understood and followed by all to protect sensitive information from the time it is captured by the VA until it is finally disposed of. Each of these in-depth programs have controls that overlap and are assessed annually to ensure requirements are being met and assist staff with questions concerning the proper handling of information.

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

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
VISTA	Patient Identification	Patient Demographics (Name, Age, Date of Birth, Sex, SSN, Marital Status, Phone Number, Home Address,)	Secure Socket Layer (SSL), HL7
VASLC FUJI CardioPACS	Patient Care	Non-Radiological DICOM (Digital Imaging and Communications in Medicine) Images	Secure Socket Layer (SSL), DICOM
VHAV19 AGFA EI PACS	Patient Care	Radiological DICOM (Digital Imaging and Communications in Medicine) Images	Secure Socket Layer (SSL), DICOM
VA OIT Gold Image Workstations	Patient Care	Patient Demographics (Name, Age, Date of Birth, Sex, SSN, Marital Status, Phone Number, Home Address) Radiological and Non-Radiological DICOM (Digital Imaging and Communications in Medicine) Images	Hypertext Transfer Protocol Secure (HTTPS)
Clinical/ Diagnostic VA Staff	Patient Care	Patient Demographics (Name, Age, Date of Birth, Sex, SSN, Marital Status, Phone Number, Home Address) Radiological and Non-Radiological DICOM (Digital Imaging and Communications in Medicine) Images	Hypertext Transfer Protocol Secure (HTTPS)

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: Unauthorized Access to data could provide bad actors with PII and PHI elements for patients receiving care at VA.

Mitigation: All system access is granted by PIV (2FA) and membership in AD groups. AD group membership managed by designated and trusted VA personnel. All administrative access is managed by VA EPAS and group membership is managed by designated trusted VA personnel.

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

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
N/A	N/A	N/A	N/A	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: None

Mitigation: N/A

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 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.

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.”

Notice is also provided in the Federal Register with the publication of the SORN: SORN 24VA10A7 /85 FR 62406 (Patient Medical Records-VA)

<https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf>

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

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

<https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.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)

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: SORN 24VA10A7 /85 FR 62406 (Patient Medical Records-VA)
<https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.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.

VHA Handbook 1605.1 Appendix D ‘Privacy and Release Information’, section 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual’s individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

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.

The VHA Notice of Privacy Practices provides information to a patient (i.e., Veteran) on their right to consent to uses of their information. The Notice states “To request a restriction, you must submit a written request that identifies the information you want restricted, when you want it to be restricted, and the extent of the restrictions. All requests to restrict use or disclosure should be submitted to the facility Privacy Officer at the VHA health care facility that provided or paid for your care.”

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: Information stored without notification could become targeted in an attack and exposed.

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

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.

Other disclosures of non-covered PII and PHI may be requested in accordance with the Freedom of Information Act (FOIA). To submit a FOIA request an entity must register with PAL and submit a complete request through VA's electronic FOIA portal.

In the course of normal system maintenance and administration credentialed VA employees and contractors may interact with PII and PHI, these individuals are charged to comply with VA Privacy Act policies requiring employees to only view sensitive data in the discharge of their duties as VA personnel.

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)?

AGFA PACS VNA 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?

This 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.

As a customer of VA VISTA/CPRS this system could receive erroneous or inaccurate information from the parent system via VISTA Integration. If inaccurate or erroneous information were transmitted to this system from VISTA/ CPRS the information would need to be corrected in VISTA/CPRS. 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 Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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.

A Notification for correcting the information must be accomplished by informing the individual to whom the record pertains by mail. The individual making the amendment must be advised in

writing that the record has been amended and provided with a copy of the amended record. The System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee, must notify the relevant persons or organizations whom had previously received the record about the amendment. If 38 U.S.C. 7332-protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

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 ensure data accuracy.***

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

Individuals may seek records and corrections to records by written request

[VHA Form 10-5345a Fill-revision.pdf \(va.gov\)](#)

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 risk of incorrect information in an individual's records is mitigated by authenticating information, when possible. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments. The NOPP discusses the process for requesting an amendment to one's records. The 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 MyHealthVet 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 receive access to the system in two ways depending on level of access. System access for system and database administration is managed through the EPAS process and membership in security groups. Access for user access is managed through membership in AD groups. All access is achieved via two factor or multifactor authentication.

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 other agencies will have access to this system.

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.

System Administrator: Access to servers and cloud environment to perform regular maintenance on servers and applications.

Database Administrator: Access to database and cloud environment to perform health checks and modifications to the database.

General User: Read Only access to view PHI within a WebApp utility.

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 incidental access to PII in the course of their work supporting and maintaining the system. The contractors have a BAA.

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.

Prior to receiving access, the user must complete and sign User Access Request Form. The user must complete, acknowledge, and electronic signs he/she will abide by the VA Rules of Behavior. The user also must complete mandatory HIPAA and security and privacy awareness training.

8.4 Has Authorization and Accreditation (A&A) been completed for the system? No

8.4a If Yes, provide:

- 1. The Security Plan Status:*
- 2. The System Security Plan Status Date:*
- 3. The Authorization Status:*
- 4. The Authorization Date:*
- 5. The Authorization Termination Date:*
- 6. The Risk Review Completion Date:*
- 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.

9/30/2024

Section 9 – Technology Usage

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

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

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

This system utilizes the VAEC's AWS environment in a Platform as a Service (PaaS) 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.

N/A

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

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

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

N/A

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

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

N/A

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

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

The 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
SE	Security
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	Transparency
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	Use Limitation
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Privacy Officer, John McKinney

Information Systems Security Officer, Eduardo Lorenzo

Information Systems Owner, Kelly Luu

APPENDIX A-6.1

SORN 24VA10A7 /85 FR 62406 (Patient Medical Records-VA) <https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf>

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

HELPFUL LINKS:

General Records Schedule

<https://www.archives.gov/records-mgmt/grs.html>

National Archives (Federal Records Management):

<https://www.archives.gov/records-mgmt/grs>

VA Publications:

<https://www.va.gov/vapubs/>

VA Privacy Service Privacy Hub:

<https://dvagov.sharepoint.com/sites/OITPrivacyHub>

Notice of Privacy Practice (NOPP):

[VHA Notice of Privacy Practices](#)

[VHA Handbook 1605.04: Notice of Privacy Practices](#)