

PIA SECTIONS 1 - 4

Part I. Project Identification and Determination of PIA Requirement

1. PROJECT IDENTIFICATION:

1.1) Project Basic Information:

1.1.a) Project or Application Name:

VistA Imaging-2009

1.1.b) OMB Unique Project Identifier:

029-00-01-11-01-1181-00

1.1.c) Project Description

*Project description is pre-populated from Exhibit 300 Part I.A.8. You will not be able to edit the description on this form.*

The VistA Imaging Project integrates state-of-the-art hardware and software to provide online patient clinical images and scanned documents to healthcare providers, increase clinician productivity, facilitate medical decision-making, and improve the quality of care for veterans. VistA Imaging captures clinical images, scanned documents, EKG waveforms and other non-textual data files and makes them part of the computerized patient record (CPRS). VistA Imaging is a windows-based, low cost imaging display software that runs on COTS workstations and is totally integrated with the other VistA healthcare applications, thus enhancing workflow. Clinical images and scanned documents linked to online medical chart information are essential in providing healthcare in VHA's distributed environment and in complying with hospital accreditation regulations. With the advent of VistA Imaging, the VA now leads the nation in integrating diagnostic images into the electronic health record. The VistA Imaging project has installed or upgraded VistA Imaging capabilities at all VA medical centers. Planned enhancements to VistA Imaging have provided VAMCs with the capability to view their patients' images even when stored at other VA medical centers and to see dental images online. Additional enhancements to VistA Imaging are addressed in the OMB Exhibit 300 for VistA Applications Development. The goal of this project's maintenance phase is to maintain the software and hardware of the VistA Imaging System at facilities in the field throughout the lifecycle of the project (which ends in 2011). Maintenance is provided for all VistA Imaging System components at all sites. Equipment is also upgraded, refreshed with new technology, or replaced in this phase. This project was approved by the VA CIO Council in 2001 and by the Strategic Management Committee in the second quarter of FY 2002. The VistA Imaging System application documentation was reviewed at that time and annually since then and was found to be in conformance with VHA architectural standards, the direction described in the VHA Enterprise Architecture (EA), and the standards prescribed by the Technical Reference Model/Standards Profile section of the VHA EA. The Exhibit 300s prepared for VistA Imaging have been reviewed and approved by the VA and OMB each of the past five years. VistA Imaging's next milestone review will be Milestone 4, at the end of the project.

1.1.d) Additional Project Information (Optional)

*The project description provided above should be a concise, stand-alone description of the project. Use this section to provide any important, supporting details.*

1.2) Contact Information:

1.2.a) Person completing this document:	Dayhoff, Ruth E (M.D.)
Title:	Director, Imaging
Organization:	VistA Imaging, HPS, VHA
Telephone Number:	301-734-0112
Email Address:	ruth.dayhoff@va.gov
1.2.b) Project Manager:	Ng, Daniel

<b>Title:</b>	Director, Project Management
<b>Organization:</b>	OI&T Business Operations
<b>Telephone Number:</b>	760.643.2031
<b>Email Address:</b>	daniel.ng@va.gov
<b>1.2.c) Staff Contact Person:</b>	Frank, Stuart
<b>Title:</b>	
<b>Organization:</b>	VistA Imaging, HSDD, VHA
<b>Telephone Number:</b>	301 734-0153
<b>Email Address:</b>	stuart.frank@va.gov

*ADDITIONAL INFORMATION: If appropriate, provide explanation for limited answers, such as the development stage of project.*

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

## 2. DETERMINATION OF PIA REQUIREMENTS:

*A privacy impact assessment (PIA) is required for all VA projects with IT systems that collect, maintain, and/or disseminate personally identifiable information (PII) of the public, not including information of Federal employees and others performing work for VA (such as contractors, interns, volunteers, etc.), unless it is a PIV project. All PIV projects collecting any PII must complete a PIA. PII is any representation of information that permits the identity of an individual to be reasonably inferred by either direct or indirect means. Direct references include: name, address, social security number, telephone number, email address, financial information, or other identifying number or code. Indirect references are any information by which an agency intends to identify specific individuals in conjunction with other data elements. Examples of indirect references include a combination of gender, race, birth date, geographic indicator and other descriptors.*

*2.a) Will the project collect and/or maintain personally identifiable information of the public in IT systems?*

Yes

*2.b) Is this a PIV project collecting PII, including from Federal employees, contractors, and others performing work for VA?*

No

*If "YES" to either question then a PIA is required for this project. Complete the remaining questions on this form. If "NO" to both questions then no PIA is required for this project. Skip to section 14 and affirm.*

*ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)*

## Part II. Privacy Impact Assessment

### 3. PROJECT DESCRIPTION:

*Enter the information requested to describe the project.*

*3.a) Provide a concise description of why personal information is maintained for this project, such as determining eligibility for benefits or providing patient care.*

Patients' medical images and documents must be identified with a defined set of patient identification information so that healthcare provided by the VA will be appropriate for that particular patient and that no identification errors will occur.

3.b) What specific legal authorities authorize this project, and the associated collection, use, and/or retention of personal information?

Vista Imaging is authorized by Title 38, United States Code, Section 501(b) and Section 304 and Section 7301(a). VHA Directive 2001-045 also mandated the implementation of Vista Imaging Core Infrastructure and Document Imaging. In 2005, the VA Undersecretary for Health directed that images originating in commercial systems within the VA be stored in Vista Imaging.

3.c) Identify, by selecting the appropriate range from the list below, the approximate number of individuals that (will) have their personal information stored in project systems.

1,000,000 - 9,999,999

3.d) Identify what stage the project/system is in: (1) Design/Planning, (2) Development/Implementation, (3) Operation/Maintenance, (4) Disposal, or (5) Mixed Stages.

(3) Operation/Maintenance

3.e) Identify either the approximate date (MM/YYYY) the project/system will be operational (if in the design or development stage), or the approximate number of years that the project/system has been in operation.

Vista Imaging has been operational since 2002, and has been fully implemented since 2004.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

#### 4. SYSTEM OF RECORDS:

The Privacy Act of 1974 (Section 552a of Title 5 of the United States Code) and VA policy provide privacy protections for employee or customer information that VA or its suppliers maintain in a System of Records (SOR). A SOR is a file or application from which personal information is retrieved by an identifier (e.g. name, unique number or symbol). Data maintained in a SOR must be managed in accordance with the requirements of the Privacy Act and the specific provisions of the applicable SOR Notice. Each SOR Notice is to be published in the Federal Register. See VA Handbook 6300.5 "Procedures for Establishing & Managing Privacy Act Systems Of Records", for additional information regarding Systems of Records.

4.a) Will the project or application retrieve personal information on the basis of name, unique number, symbol, or other identifier assigned to the individual?

If "No" then skip to section 5, 'Data Collection'.

Yes

4.b) Are the project and/or system data maintained under one or more approved System(s) of Records?

IF "No" then SKIP to question 4.c.

Yes

4.b.1) For each applicable System of Records, list:

(1) The System of Records identifier (number),

79VA19, 24VA19

(2) The name of the System of Records, and

Veterans Health Information Systems and Technology Architecture (Vista), Patient medical Records

(3) Provide the location where the specific applicable System of Records Notice(s) may be accessed (include the URL).

[http://vaww.vhaco.va.gov/privacy/Update\\_SOR/SOR24VA19.pdf](http://vaww.vhaco.va.gov/privacy/Update_SOR/SOR24VA19.pdf)

[http://www.va.gov/privacy/SystemsOfRecords/2001\\_Privacy\\_Act\\_GPO\\_SOR\\_compilation.pdf](http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf)

IMPORTANT: For each applicable System of Records Notice that is not accessible via a URL: (1) Provide a concise explanation of why the System of Records Notice is not accessible via a URL in the "Additional Information" field at the end of this section, and (2) Send a copy of the System of Records Notice(s) to the Privacy Service.

4.b.2) Have you read, and will the application comply with, all data management practices in the System of Records Notice(s)?

Yes

4.b.3) Was the System(s) of Records created specifically for this project, or created for another project or system?

Created for another project or system

If created for another project or system, briefly identify the other project or system.

VistA Imaging is part of the larger VistA System of Records which handles medical information for the Dept. of Veterans Affairs.

4.b.4) Does the System of Records Notice require modification?

If "No" then skip to section 5, 'Data Collection'.

Modification of the System of Records is NOT Required.

4.b.5) Describe the required modifications.

4.c) If the project and/or system data are not maintained under one or more approved System(s) of Records, select one of the following and provide a concise explanation.

Explanation:

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## PIA SECTION 5

### Project Name

VistA Imaging-2009

## 5. DATA COLLECTION:

### 5.1 Data Types and Data Uses

Identify the types of personal information collected and the intended use(s) of that data:

a) Select all applicable data types below. If the provided data types do not adequately describe a specific data collection, select the "Other Personal Information" field and provide a description of the information.

b) For each selected data type, concisely describe how that data will be used.

*Important Note: Please be specific. If different data types or data groups will be used for different purposes or multiple purposes, specify. For example: "Name and address information will be used to communicate with individuals about their benefits, while Name, Service, and Dependent's information will be used to determine which benefits individuals will be eligible to receive. Email address will be used to inform individuals about new services as they become available."*

Yes	<b>Veteran's or Primary Subject's Personal Contact Information (name, address, telephone, etc.)</b>
-----	---

Specifically identify the personal information collected, and describe the intended use of the information.

The primary data that is collected is medical images, identified by patient. Medical images are collected to allow VHA clinicians to provide quality patient care. Patient images must be identified to ensure that the correct patient is treated in accordance with their particular medical condition(s). Patients' medical images and documents must be identified with a defined set of patient identification information so that no identification errors will occur. Identification information is in the form of pointers to a master file maintained by the VA's hospital information system (VistA). Information (such as name, social security number, and VA control number) is also stored in the image headers.

Yes	<b>Other Personal Information of the Veteran or Primary Subject</b>
-----	---

*Specifically identify the personal information collected, and describe the intended use of the information.*

VistA Imaging may also store photographs of patients' faces. This information is used to verify patient identification. This is particularly important when dementia patients wander away from their hospital beds and must be returned to their ward.

No	<b>Dependent Information</b>
----	------------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

No	<b>Service Information</b>
----	----------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

Yes	<b>Medical Information</b>
-----	----------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

The primary data that is collected is medical images, identified by patient in each image file. Medical images are collected to allow VHA clinicians to provide quality patient care. Patient images must be identified to ensure that the correct patient is treated in accordance with their particular medical condition(s). Patients' medical images and documents must be identified with a defined set of patient identification information so that no identification errors will occur.

No	<b>Criminal Record Information</b>
----	------------------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

No	<b>Guardian Information</b>
----	-----------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

No	<b>Education Information</b>
----	------------------------------

Specifically identify the personal information collected, and describe the intended use of the information.

--	--

No	<b>Rehabilitation Information</b>
----	-----------------------------------

Specifically identify the personal information collected, and describe the intended use of the information.

--	--

Yes	<b>Other Personal Information (specify):</b>
-----	--

The "Other Personal Information" field is intended to allow identification of collected personal information that does not fit the provided categories. If personal information is collected that does not fit one of the provided categories, specifically identify this information and describe the intended use of the information.

Under 24VA 19 we collect ethic and gender information

*ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)*

Vista Imaging collects medical images for use in the medical treatment of its veteran patients. These are part of each patient's medical record and are used to document the patient's condition, treatment, and progress. It is very important that medical images be labeled with the patient's identifying information to be sure that treatment is provided to the correct patient for the medical condition seen in the images and diagnosed from the procedures and tests. The identifying information is not used independently of the images.

## 5.2 Data Sources

Identify the source(s) of the collected information.

a) Select all applicable data source categories provided below.

b) For each category selected:

i) Specifically identify the source(s) - identify each specific organization, agency or other entity that is a source of personal information. ii) Provide a concise description of why information is collected from that source(s). iii) Provide any required additional clarifying information.

Your responses should clearly identify each source of personal information, and explain why information is obtained from each identified source. (Important Note: This section addresses sources of personal information; Section 6.1, "User Access and Data Sharing" addresses sharing of collected personal information.)

Note: PIV projects should use the "Other Source(s)" data source.

Yes	<b>Veteran Source</b>
-----	-----------------------

Provide a concise description of why information is collected from Veterans. Provide any required additional, clarifying information.

Vista Imaging obtains several kinds of information from veterans. Some information is provided by the veteran directly, such as documents to be included in the patient's chart or images brought from an outside hospital on CDs. Medical image information is acquired from the veteran through the use of various medical devices, such as CT scanners or digital cameras. Each of these is described below.

VistA Imaging stores scanned documents related to the veteran's patient record. These include documents signed by the veteran, documents about the veteran's healthcare, and documents provided by the veteran related to treatment received at non-VA facilities. These documents are used by clinicians providing medical care to the veteran. Some administrative documents related to veterans' healthcare is also stored.

VistA Imaging stores digital medical images from veterans, like xrays, photos of skin lesions, microscope slide images, scanned reports of procedures, etc. The source of the information is the Veteran. The veteran's images are acquired using a device like an xray machine, camera, endoscope, retinal camera, or image capture workstation. Therefore, a digitizing system is an intermediary source of the information. This intermediary source transmits the veterans digital images to the VistA Imaging storage device. In some cases, patient images or patient reports are obtained from other medical facilities outside the VA. These images and reports are generally provided by the patient themselves.

No	<b>Public Source(s)</b>
----	-------------------------

*i) Specifically identify the Public Source(s) - identify the specific organization(s) or other entity(ies) that supply personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.*

Yes	<b>VA Files and Databases</b>
-----	-------------------------------

*i) Specifically identify each VA File and/or Database that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.*

Patients' medical images and documents must be identified with a defined set of patient identification information. Some identification information is in the form of pointers to a master file maintained by the VA's hospital information system (VistA).

Yes	<b>Other Federal Agency Source(s)</b>
-----	---------------------------------------

Currently, images are routinely sent from the Dept. of Defense to the VA for a subset of patients - those who have sustained polytrauma injuries. At the present time, radiology images and scanned medical records documents are being received from DoD. There are future plans to expand prototype work on bi-directional image sharing. This will allow clinicians treating shared VA/DoD patients to view certain radiology images (CT, CR, MR).

*i) Specifically identify each Federal Agency that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.*

v(1) Dept. of Veterans Affairs and Dept. of Defense are sources of personal information. (2) This information is collected in order to provide images and scanned documents needed for medical treatment for the individual patients.

No	<b>State Agency Source(s)</b>
----	-------------------------------

i) Specifically identify each State Agency that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.

No	<b>Local Agency Source(s)</b>
----	-------------------------------

i) Specifically identify each Local Agency (Government agency other than a Federal or State agency) that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.

No	<b>Other Source(s)</b>
----	------------------------

i) If the provided Data Source categories do not adequately describe a source of personal information, specifically identify and describe each additional source of personal information. ii) For each identified data source, provide a concise description of why information is collected from that source. iii) Provide any required additional, clarifying information.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

**5.3 Collection Methods**

Identify and describe how personal information is collected:

a) Select all applicable collection methods below. If the provided collection methods do not adequately describe a specific data collection, select the "Other Collection Method" field and provide a description of the collection method. b) For each collection method selected, briefly describe the collection method, and provide additional information as indicated.

No	<b>Web Forms:</b>	Information collected on Web Forms and sent electronically over the Internet to project systems.
----	-------------------	--

Identify the URL(s) of each Web site(s) from which information will be submitted, and the URL(s) of the associated privacy statement. (Note: This question only applies to Web forms that are submitted online. Forms that are accessed online, printed and then mailed or faxed are considered "Paper Forms.")

Yes	<b>Paper Forms:</b>	Information collected on Paper Forms and submitted personally, submitted via Postal Mail and/or submitted via Fax Machine.
-----	---------------------	--

Identify and/or describe the paper forms by which data is collected. If applicable, identify standard VA forms by form number.

Vista Imaging scans any paper forms related to the veteran's patient record, as determined by the healthcare provider. These documents are used by clinicians providing medical care to the veteran.

No	<b>Electronic File Transfer:</b>	Information stored on one computer/system (not entered via a Web Form) and transferred electronically to project IT systems.
----	----------------------------------	--

*Describe the Electronic File Transfers used to collect information into project systems. (Note: This section addresses only data collection – how information stored in project systems is acquired. Sharing of information stored in project systems and data backups are addressed in subsequent sections.)*

Yes	<b>Computer Transfer Device:</b>	Information that is entered and/or stored on one computer/ system and then transferred to project IT systems via an object
		or device that is used to store data, such as a CD-ROM, floppy disk or tape.

*Describe the type of computer transfer device, and the process used to collect information.*

Digital medical images are acquired through standard image interfaces from medical devices or from cameras. Images are identified with the patient's medical record through use of the hospital information system database. In some cases, images or reports are provided on compact discs by the patients themselves; these are imported through the VistA Imaging interface.

No	<b>Telephone Contact:</b>	Information is collected via telephone.
----	---------------------------	---

*Describe the process through which information is collected via telephone contacts.*

No	<b>Other Collection Method:</b>	Information is collected through a method other than those listed above.
----	---------------------------------	--

*If the provided collection method categories do not adequately describe a specific data collection, select the "Other Collection Method" field and specifically identify and describe the process used to collect information.*

*ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)*

#### 5.4 Notice

*The Privacy Act of 1974 and VA policy requires that certain disclosures be made to data subjects when information in identifiable form is collected from them. The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.*

*5.4.a) Is personally identifiable information collected directly from individual members of the public and maintained in the project's IT systems?*

Yes

Note: If you have selected NO above, then SKIP to Section 5.5, 'Consent'.

5.4.b) Is the data collection mandatory or voluntary?

Voluntary

5.4.c) How are the individuals involved in the information collection notified of the Privacy Policy and whether provision of the information is mandatory or voluntary?

Individuals choose to consent to the performance of a medical test or procedure. This consent includes the capture and storage of required images with the patient's electronic medical record.

5.4.d) Is the data collection new or ongoing?

Ongoing

5.4.e.1) If personally identifiable information is collected online, is a privacy notice provided that includes the following elements? (Select all applicable boxes.)

Yes	<b>Not applicable</b>
No	<b>Privacy notice is provided on each page of the application.</b>
No	<b>A link to the VA Website Privacy Policy is provided.</b>
No	<b>Proximity and Timing: the notice is provided at the time and point of data collection.</b>
No	<b>Purpose: notice describes the principal purpose(s) for which the information will be used.</b>
No	<b>Authority: notice specifies the legal authority that allows the information to be collected.</b>
No	<b>Conditions: notice specifies if providing information is voluntary, and effects, if any, of not providing it.</b>
No	<b>Disclosures: notice specifies routine use(s) that may be made of the information.</b>

5.4.e.2) If necessary, provide an explanation on privacy notices for your project:

Patient does not enter data using the VistA Imaging application. Documents are scanned into VistA Imaging by VHA staff.

5.4.f) For each type of collection method used (identified in Section 5.3, "Collection Method"), explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

Note: if PII is transferred from other projects, explain any agreements or understandings regarding notification of subjects.

No	<b>Web Forms:</b>
----	-------------------

Explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

Yes	<b>Paper Forms:</b>
-----	---------------------

Explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

N/A -- patient does not enter data using the VistA Imaging application. Documents are scanned into VistA Imaging by VHA staff.

No	<b>Electronic File Transfer:</b>
----	----------------------------------

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to notify subjects regarding:

a) What they will be told about the information collection? b) How the message will be conveyed (e.g. written notice, electronic notice if web-based collection, etc.)? c)How a privacy notice is provided?

Yes	<b>Computer Transfer Device:</b>
-----	----------------------------------

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to notify subjects regarding:

a) What they will be told about the information collection? b) How the message will be conveyed (e.g. written notice, electronic notice if web-based collection, etc.)? c)How a privacy notice is provided?

Patient does not enter data using the VistA Imaging application. Images are captured from medical devices into VistA Imaging by VHA staff. When a procedure is performed on a patient, an informed consent form is signed by the patient.

No	<b>Telephone:</b>
----	-------------------

Explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

No	<b>Other Method:</b>
----	----------------------

Explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

### 5.5 Consent For Secondary Use of PII:

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

5.5.a) Will personally identifiable information be used for any secondary purpose?

Note: If you have selected No above, then SKIP to question 5.6, "Data Quality."

No

5.5.b) Describe and justify any secondary uses of personal information.

5.5.c) For each collection method identified in question 5.3, "Collection Method," describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

Some examples of consent methods are: (1) Approved OMB consent forms and (2) VA Consent Form (VA Form 1010EZ). Provide justification if no method of consent is provided.

	<b>Web Forms:</b>
--	-------------------

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

	<b>Paper Forms:</b>
--	---------------------

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

Scanned medical record documents are required to be part of the patient's electronic medical record. Individuals may grant consent for use of their images outside of patient care.

	<b>Electronic File Transfer:</b>
--	----------------------------------

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to provide the following:

a) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. b) The opportunities individuals have to grant consent for particular uses of the information. c) How individuals may grant consent.

	<b>Computer Transfer Device:</b>
--	----------------------------------

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to provide the following:

a) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. b) The opportunities individuals have to grant consent for particular uses of the information. c) How individuals may grant consent.

Medical images are acquired from medical devices used to perform procedures on patients. Patients must sign consent forms for these procedures. Individuals may grant consent for use of their images outside of patient care.

	<b>Telephone Contact Media:</b>
--	---------------------------------

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

	<b>Other Media</b>
--	--------------------

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## 5.6 Data Quality

5.6.a) Explain how collected data are limited to required elements:

Specific fields are provided for information input. Various checks including length and data type are performed during input.

5.6.b) How is data checked for completeness?

VistA Imaging provides input checks on data collected. It also has an integrity checking function that allows scanning of data on file for internal consistency within VistA.

5.6.c) What steps or procedures are taken to ensure the data are current and not out of date?

The VistA hospital information system maintains current patient information in files used by VistA Imaging. This information is used to identify the patient. It is not appropriate to keep patient information on scanned documents or reports up-to-date, as they must reflect the state of the record at the time the document was created. Dates of procedure, record creation, and capture are made available to the user.

5.6.d) How is new data verified for relevance, authenticity and accuracy?

A quality check is performed on scanned documents and captured images before they are saved. Images can be re-captured if quality is not adequate.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

**PIA SECTIONS 6 - 13**

**Project Name**

VistA Imaging-2009

**6. Use and Disclosure**

**6.1 User Access and Data Sharing**

*Identify the individuals and organizations that have access to system data.*

--> *Individuals - Access granted to individuals should be limited to the data needed to perform their assigned duties. Individuals with access to personal information stored in project system must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to prevent as well as detect unauthorized access and browsing.*

--> *Other Agencies – Any Federal, State or local agencies that have authorized access to collected personal information must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to protect personal information.*

--> *Other Systems – Information systems of other programs or projects that interface with the information system(s) of this project must be identified and the transferred data must be defined. Also, the controls that are in place to ensure that only the defined data are transmitted must be defined.*

6.1.a) *Identify all individuals and organizations that will have access to collected information. Select all applicable items below.*

**All access is controlled through user logon privileges and assigned keys.**

Yes	<b>System Users</b>
-----	---------------------

Yes	<b>System Owner, Project Manager</b>
-----	--------------------------------------

Yes	<b>System Administrator</b>
-----	-----------------------------

Yes	<b>Contractor</b>
-----	-------------------

*If contractors to VA have access to the system, describe their role and the extent of access that is granted to them. Also, identify the contract(s) that they operate under.*

Contractors provide customer support services for VistA Imaging System. The current contract is with CACI and with Hewlett Packard. These will change next month; CACI and HP are the current contractors.

No	<b>Internal Sharing: Veteran Organization</b>
----	---

*If information is shared internally, with other VA organizations identify the organization(s). For each organization, identify the information that is shared and for what purpose.*

No	<b>Other Veteran Organization</b>
----	-----------------------------------

If information is shared with a Veteran organization other than VA, identify the organization(s). For each organization, identify the information that is shared and for what purpose.

Yes	Other Federal Government Agency
-----	---------------------------------

If information is shared with another Federal government agency(ies), identify the agency(ies). For each organization, identify the information that is shared and for what purpose.

DOD. Medical images for treatment of patients.

No	State Government Agency
----	-------------------------

If information is shared with a State government agency(ies), identify the agency(ies). For each organization, identify the information that is shared and for what purpose.

No	Local Government Agency
----	-------------------------

If information is shared with a local government agency(ies), identify the agency(ies). For each organization, identify the information that is shared and for what purpose.

Yes	Other Project/ System
-----	-----------------------

If information is shared with other projects or systems:

1) Identify the other projects and/or systems, and briefly describe the data sharing. 2) For each project and/or system with which information will be shared, identify the information that will be shared with that project or system. 3) For each project and/or system with which information will be shared, describe why information is shared. 4) For each project and/or system with which information will be shared, describe who will be responsible for protecting the privacy rights of the individuals whose data will be shared across this interface.

Medical images are sometimes shared with commercial imaging systems operating within VA and with telemedicine systems operating outside VA. In any case, there is an appropriate HIPAA agreement in place.

No	Other User(s)
----	---------------

If information is shared with persons or organization(s) that are not described by the categories provided, use this field to identify and describe what other persons or organization(s) have access to personal information stored on project systems. Also, briefly describe the data sharing.

6.1.a.1) Describe here who has access to personal information maintained in project's IT systems:

VHA clinicians and staff have access to patients' personal information for patient care purposes.

6.1.b) How is access to the data determined?

Users access to image data is determined based on their role in the patient's care. Medical facilities identify criteria

required for each applicable role and assign electronic access keys. In particular, the VistA Imaging System supports access keys for viewing images, acquiring images for specific specialties, and administering the system. The VistA Imaging access keys distinguish between administrative and clinical image/document access.

6.1.c) Are criteria, procedures, controls, and responsibilities regarding access documented? If so, identify the documents.

Yes Privacy Policy 1605.1

6.1.d) Will users have access to all data on the project systems or will user access be restricted? Explain.

User access is restricted based on electronic access keys and assigned menu options. These keys and menu option assignments allow user access to be restricted based on administrative or clinical duties, specialty of provider, or administrative functions to be performed.

6.1.e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by those having access? (Please list processes and training materials that specifically relate to unauthorized browsing)

There are controls in place to prevent misuse. Access to patient information is logged electronically. Warnings are displayed for sensitive patients. If a clinician or other user must access the patient's information, their access will be logged electronically and follow-up will be done by the Security Officer. All VHA employees are required to complete privacy training yearly.

6.1.f) Is personal information shared (is access provided to anyone other than the system users, system owner, Project Manager, System Administrator)? (Yes/No)

Yes

Note: If you have selected No above, then SKIP to question 6.2, "Access to Records and Requests for Corrections".

6.1.g) Identify the measures taken to protect the privacy rights of the individuals whose data will be shared.

Sharing is for the purpose of providing medical care. There is an appropriate HIPAA agreement in place.

6.1.h) Identify who is responsible, once personal information leaves your project's IT system(s), for ensuring that the information is protected.

All VistA applications sharing the data are responsible for restricting access to this information. The Medical Center Directors and Program Office Directors are responsible for ensuring HIPAA and privacy act compliance.

6.1.i) Describe how personal information that is shared is transmitted or disclosed.

Information is transmitted via the DICOM standard, in accordance with the government-wide Consolidated Health Informatics Initiative.

6.1.j) Is a Memorandum of Understanding (MOU), contract, or any other agreement in place with all external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared? If an MOU is not in place, is the sharing covered by a routine use in the System of Records Notice? If not, explain the steps being taken to address this omission.

Yes

6.1.k) How is the shared information secured by the recipient?

The recipient is under the same HIPAA requirements as the VA.

6.1.l) What type of training is required for users from agencies outside VA prior to receiving access to the information?

The Dept. of Defense is responsible for training their employees in secure use of their workstations.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## 6.2 Access to Records and Requests for Corrections

The Privacy Act and VA policy provide certain rights and mechanisms by which individuals may request access to and amendment of information relating to them that is retained in a System of Records.

6.2.a) How can individuals view instructions for accessing or amending data related to them that is maintained by VA? (Select all applicable options below.)

No	<b>The application will provide a link that leads to their information.</b>
No	<b>The application will provide, via link or where data is collected, written instructions on how to access/amend their information.</b>

No	<b>The application will provide a phone number of a VA representative who will provide instructions.</b>
Yes	<b>The application will use other method (explain below).</b>
No	<b>The application is exempt from needing to provide access.</b>

6.2.b) What are the procedures that allow individuals to gain access to their own information?

The individual may file a request to access their own information.

6.2.c) What are the procedures for correcting erroneous information?

The individual may file a request for correction of his or her medical record.

6.2.d) If no redress is provided, are alternatives available?

N/A

6.2.e) Provide here any additional explanation; if exempt, explain why the application is exempt from providing access and amendment.

VistA Imaging does not interact with the veteran directly. The VA provides information about Release of Information (ROI) on its webpage. The process for release of medical record information is handled by the ROI office in each medical center, not by individual software applications. Images and scanned documents are handled by this process. VistA Imaging provides functions that are used by ROI staff for this purpose.

*ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)*

## 7 Retention and Disposal

By completing this section, you provide documented assurance that proper data retention and disposal practices are in place.

The "Retention and disposal" section of the applicable System of Records Notice(s) often provides appropriate and sufficiently detailed documented data retention and disposal practices specific to your project.

VA HBK 6300.1 Records Management Procedures explains the Records Control Schedule procedures.
<b>System of Records Notices may be accessed via:</b>
<a href="http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm">http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm</a>
or
<a href="http://vaww.va.gov/foia/err/enhanced/privacy_act/privacy_act.html">http://vaww.va.gov/foia/err/enhanced/privacy_act/privacy_act.html</a>
For VHA projects, VHA Handbook 1907.1 (Section 6j) and VHA Records Control Schedule 10-1 provide more general guidance.
<b>VHA Handbook 1907.1 may be accessed at:</b>
<a href="http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=434">http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=434</a>
For VBA projects, Records Control Schedule (RCS) VB-1 provides more general guidance. VBA Records Control Schedule (RCS) VB-1 may be accessed via the URL listed below.
<a href="http://www.warms.vba.va.gov/20rcs.html">Start by looking at the http://www.warms.vba.va.gov/20rcs.html</a>

7.a) What is the data retention period? Given the purpose of retaining the information, explain why the information is needed for the indicated period.

The VA has detailed retention requirements for different kinds of images. We follow RCS 10-1. VistA Imaging retains

currently retains all images. We are performing a study to explore whether some images can be eliminated on an earlier schedule.

7.b) What are the procedures for eliminating data at the end of the retention period?

The VA has procedures for eliminating stored data when storage devices are disposed of. These procedures are followed when media, such as optical disk platters, must be disposed of.

7.c) Where are procedures documented?

Procedures for data elimination are detailed in the following documents:  
 VistA Imaging System Security Plan  
 VistA Imaging Security Plan, Site-Specific Security Controls, section 3.3.  
 VA CIO Memorandum titled "Policy Regarding Removal of Sensitive Data from Electronic Storage Media"

7.d) How are data retention procedures enforced?

VistA Imaging integrity checking software is used to ensure that no images are lost.

7.e) If applicable, has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Yes

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## 8 SECURITY

OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, (OMB M-03-22) specifies that privacy impact assessments must address how collected information will be secured.

### 8.1 General Security Measures

8.1.a) Per OMB guidance, citing requirements of the Federal Information Security Management Act, address the following items (select all applicable boxes.):

Yes	The project is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured.
Yes	The project has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.
Yes	Security monitoring, testing, and evaluating are conducted on a regular basis to ensure that controls continue to work properly, safeguarding the information.

8.1.b) Describe the security monitoring, testing, and evaluating that is conducted on a regular basis:

OCIS manages and monitors Department-wide security solutions, such as anti-virus protection, authentication, independent vulnerability scanning and penetration testing, and intrusion detection systems. Each year an annual security self-assessment survey is conducted as part of the VA's IT security framework, with this project completing its FISMA Survey in July 2005. The results of the survey are used by the VA CIO to develop Department-wide remediation priorities. Additionally, the VistA Imaging program manager uses the survey results to evaluate the adequacy of safeguards on the system, and ensure that the system is adequately funded for security needs. The VistA Imaging Security Plan is updated periodically to reflect the results of IT security controls adopted for implementation through the annual FISMA Survey. At the close of the survey period, appendices of security controls selected for the system, as well as controls that are either temporarily or permanently suspended as a result of the Program Manager's risk-based decisions, are generated. VistA Imaging is a medical device regulated by the Food and Drug Administration (FDA), and therefore undergoes rigorous testing of the VistA Imaging device. VistA Imaging has gone through the C&A process, including testing of operational and management security controls. IT security for medical devices is also provided through education of system owners and operators relating to the risks associated with these devices being connected to VA networks, as well as some operational and management controls. In addition, the OCIS performs onsite review and inspection division (RID) audits at VHA facilities including testing of the effectiveness of certain management and operational IT security controls related

to facility systems, including VistA Imaging and other IT medical devices. Any noted deficiencies are entered into the FISMA POA&M database. It is noted that OCIS's Health Information Security Division (HISD) was established to perform security assessments of medical devices and identify methodologies to secure medical devices on VA networks, to include implementation of VLANs and working with medical device vendors to encourage the implementation of security controls, consistent with FDA certification requirements. VA's Network and Security Operations Center (NSOC) monitors VA networks through IDS sensors, ensuring that suspicious events are detected, analyzed, and handled appropriately. The NSOC works collaboratively with Information Security Officers (ISOs) at all VA locations to report and/or follow up on suspicious network activity captured by IDS sensors. The VA-CIRC is the central coordinating and response office for all cyber security incidents affecting the VA. The VA-CIRC identifies, validates, and directs all response efforts, and coordinates efforts with government incident response centers including US-CERT.

8.1.c) Is adequate physical security in place to protect against unauthorized access?

Yes

## 8.2 Project-Specific Security Measures

8.2.a) Provide a specific description of how collected information will be secured.

- A concise description of how data will be protected against unauthorized access, unauthorized modification, and how the availability of the system will be protected.

- A concise description of the administrative controls (Security Plans, Rules of Behavior, Procedures for establishing user accounts, etc.).

- A concise description of the technical controls (Access Controls, Intrusion Detection, etc.) that will be in place to safeguard the information.

- Describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses. For example, are audit logs regularly reviewed to ensure appropriate use of information? Are strict disciplinary programs in place if an individual is found to be inappropriately using the information?

Note: Administrative and technical safeguards must be specific to the system covered by the PIA, rather than an overall description of how the VA's network is secured. Does the project/system have its own security controls, independent of the VA network? If so, describe these controls.

Specific VistA Imaging information including medical images, scanned documents, and related information will be secured as follows: 1) VistA Imaging data is protected through the use of controls such as lack of any end-user access to the image server files, image storage management protections against elimination of data, and VistA Imaging file access restriction. Project systems are protected with access controls, access monitoring, role specific access, virus protection, backup and redundancy. 2) Administrative controls that protect collected information include the use of the VistA Imaging Security Plan by medical centers, Rules of Behavior signed by those with access to the system, VA procedures for establishing user accounts on the VistA hospital information system, and yearly user training. 3) Technical controls to safeguard the information include individual access authentication, logging, password protection (content and life restricted), monitoring unsuccessful login attempts, restriction by security keys, file access restriction, session time-outs, and separation of user from data storage devices. Please see the VistA Imaging Security Plan documents for additional security details.

8.2.b) Explain how the project meets IT security requirements and procedures required by federal law.

VistA Imaging has completed the C&A process successfully. The VistA Imaging Security Plan identifies how the requirements and procedures will be addressed.

## 9. CHANGE RECORD

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, mandates that PIAs address any project/ system changes that potentially create new privacy risks. By completing this section, you provide documented assurance that significant project/ system modifications have been appropriately evaluated for privacy-related impacts.

9.a Since the last PIA submitted, have any significant changes been made to the system that might impact the privacy of people whose information is retained on project systems? (Yes, No, n/a: first PIA)

No

If no, then proceed to Section 10, "Children's Online Privacy Protection Act."

If yes, then please complete the information in the table below. List each significant change on a separate row. 'Significant changes' may include:

Conversions - when converting paper-based records to electronic systems;

Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;

Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:

- For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.

*Significant Merging* - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:

- For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.

*New Public Access* - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;

*Commercial Sources* - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);

*New Interagency Uses* - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;

*Internal Flow or Collection* - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:

- For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.

*Alteration in Character of Data* - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information);

List All Major Project/System Modification(s)	State Justification for Modification(s)	* Concisely describe:	Modification Approver	Date

\* The effect of the modification on the privacy of collected personal information

\* How any adverse effects on the privacy of collected information were mitigated.

## 10. CHILDREN'S ONLINE PRIVACY PROTECTION ACT

10.a) Will information be collected through the Internet from children under age 13?

No

If "No" then SKIP to Section 11, "PIA Considerations".

10.b) How will parental or guardian approval be obtained.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## 11. PIA CONSIDERATIONS

11) Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA. Examples of choices made include reconsideration of: collection source, collection methods, controls to mitigate misuse of information, provision of consent and privacy notice, and security controls.

Protection of privacy has always been a focus of VistA Imaging and the overall VistA System. The PIA reaffirmed the need for the protections that have been built into the VistA Imaging System.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## 12. PUBLIC AVAILABILITY

The Electronic Government Act of 2002 requires that VA make this PIA available to the public. This section is intended to provide documented assurance that the PIA is reviewed for any potentially sensitive information that should be removed from the version of the PIA that is made available to the public.

The following guidance is excerpted from M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," Section II.C.3, "Review and Publication": iii. Agencies must ensure that the PIA document and, if prepared, summary, are made publicly available (consistent with executive branch policy on the release of information about systems for which funding is proposed).

1. Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment<sup>9</sup>. Such information shall be protected and handled consistent with the Freedom of Information Act (FOIA).

2. Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds.

12.a) Does this PIA contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

No

12.b) If yes, specify:

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## 13. ACCEPTANCE OF RESPONSIBILITY AND ACKNOWLEDGEMENT OF ACCOUNTABILITY:

13.1) I have carefully reviewed the responses to each of the questions in this PIA. I am responsible for funding and procuring, developing, and integrating privacy and security controls into the project. I understand that integrating privacy and security considerations into the project may affect the development time and cost of this project and must be planned for accordingly. I will ensure that VA privacy and information security policies, guidelines, and procedures are followed in the development, integration, and, if applicable, the operation and maintenance of this application.

Yes

13.2) Project Manager/Owner Name and Date (mm/dd/yyyy)

Daniel Ng, 09/26/07

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)