

**Privacy Impact Assessment - 2008 (Form) /  
 Central Arkansas Veterans Healthcare System, Little Rock, Arkansas  
 VISTA System**

ProSight

**PRIVACY IMPACT ASSESSMENT 2008**

**Part I. Project Identification and Determination of PIA Requirement**

**1. PROJECT IDENTIFICATION:**

**1.1) Project Basic Information:**

1.1.a) Project or Application Name:

**Central Arkansas Veterans Healthcare System VISTA Legacy**

1.1.b) OMB Unique Project Identifier:

**029-00-01-11-01-1180-00**

1.1.c) Concise Project Description

*Provide a concise description of the project.*

The VistA-Legacy system is the software platform and hardware infrastructure (associated with clinical operations) on which the VHA health care facilities operate their software applications and support for E-Government initiatives. It includes the computer equipment associated with clinical operations and the employees (approximately 2500 FTE) necessary to operate the system. VistA-Legacy is a client-server system. It links the facility computer network to over 100 applications and databases. In 2006, the VistA-Legacy system supported IT services across the VA organization which had a network of 21 Veterans Integrated Service Networks (VISNs) that managed 155 medical centers, over 881 community based outpatient clinics, 46 residential rehabilitation treatment programs, 135 nursing homes, 207 readjustment counseling centers, 57 veteran benefits regional offices, and 125 national cemeteries. VistA-Legacy provides critical data that supports the delivery of healthcare to veterans and their dependants. Using the computer, the VA health care provider can access VistA-Legacy applications and meet a wide range of health care data needs. The VistA-Legacy system operates in medical centers, ambulatory and community-based clinics, nursing homes and domiciliary. The VistA-Legacy system is in the mature phase of the capital investment lifecycle.

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:**

<b>1.2.a) Person completing this document: Donna Haggard</b>	
<b>Title: Information Security Officer</b>	
<b>Organization: OI&amp;T, Field Security Operations, Field Security Service</b>	
<b>Telephone Number: 501-257-2008</b>	
<b>Email Address: donna.haggard@va.gov</b>	
<b>1.2.b) Project Manager: B.K. Hack</b>	
<b>Title: Director, IT Operations, Region 2</b>	
<b>Organization: Office of Information &amp; Technology</b>	

<b>Telephone Number: 817-385-3751</b>	
<b>Email Address: bk.hack@va.gov</b>	
<b>1.2.c) Staff Contact Person: James P. Hall</b>	
<b>Title: Facility Chief Information Officer</b>	
<b>Organization: Office of Information &amp; Technology</b>	
<b>Telephone Number: 501-257-1536</b>	
<b>Email Address: James.Hall@va.gov</b>	

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

	<b>SECTION INCOMPLETE</b>
<input type="checkbox"/>	<b>SECTION COMPLETED</b>
<input checked="" type="checkbox"/>	I have completed and reviewed my responses in this section.
<b>** NOTE:</b>	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	<b>Section Update Date</b>

**Section 1 Review:**

	<b>PRIVACY SERVICE SECTION REVIEW AND APPROVAL</b>
	The Privacy Service has not reviewed this section.
	The Privacy Service has reviewed this section. Please make the modifications described below.
<input type="checkbox"/>	The Privacy Service has reviewed and approved the responses in this section.
<b>** NOTE:</b>	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit and then select "Yes" and submit again.
	<b>Section Review Date</b>

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

Angela Waddles, Privacy Officer, 501-257-2972

**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 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 2.

2.c) Has a previous PIA been completed within the last three years?

Yes

2.d) Has any changes been made to the system since last PIA?

No

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

No

	<b>SECTION INCOMPLETE</b>
<input type="checkbox"/>	<b>SECTION COMPLETED</b>
<input checked="" type="checkbox"/>	I have completed and reviewed my responses in this section.
<b>** NOTE:</b>	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	<b>Section Update Date</b>

**Section 2 Review:**

	<b>PRIVACY SERVICE SECTION REVIEW AND APPROVAL</b>
	The Privacy Service has not reviewed this section.
	The Privacy Service has reviewed this section. Please make the modifications described below.
<input checked="" type="checkbox"/>	The Privacy Service has reviewed and approved the responses in this section.
<b>** NOTE:</b>	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit and then select "Yes" and submit again.

**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

Angela Waddles, Privacy Officer, 501-257-2972

**Part II. Privacy Impact Assessment**

**3. PROJECT DESCRIPTION:**

The purpose of NIST SP 800-60 is to address recommending the types of information and information systems to be included in each category of potential security impact. Using NIST SP800-60, 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.

All information is necessary in order to provide congressionally mandated health care for Veterans.

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

Title 38, United States Code, section 7301(a).

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.

approximately 1,000,000

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) Operations/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.

1987; approximatley 20 years.

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

	<b>SECTION INCOMPLETE</b>
X	<b>SECTION COMPLETED</b>
X	I have completed and reviewed my responses in this section.
**	<b>NOTE:</b> If you are resubmitting your updates, first select "NO Value" from the dropdown and hit submit and then select "Yes" and hit submit.
	<b>Section Update Date</b>

**Section 3 Review:**

	<b>PRIVACY SERVICE SECTION REVIEW AND APPROVAL</b>
	The Privacy Service has not reviewed this section.
	The Privacy Service has reviewed this section. Please make the modifications described below.
	The Privacy Service has reviewed and approved the responses in this section.
<b>** NOTE:</b>	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit and then select "Yes" and submit again.
	<b>Section Review Date</b>

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

Angela Waddles, Privacy Officer, 501-257-2972.

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

79VA19-VistA (Veterans Integrated System Technical Architecture)  
 23VA136 – Patient Fee Basis Medical & Pharmacy Records  
 24VA19 – Patient Medical Records  
 56VA119 – Automated Medication Processing Records  
 76VA05 - General Personnel Records  
 89VA161 – Means Test Verification Records  
 57VA125 – Voluntary Service Records  
 97VA105 – Consolidated Data Information System  
 99VA13 – Automated Safety Incident Surveillance and Tracking System (ASISTS)  
 121VA19 – National Patient Database

(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/Systemofecords.htm>

**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 specifically for this project

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

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.

N/A

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.

N/A

Explanation:

N/A

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

		<b>SECTION INCOMPLETE</b>
	X	<b>SECTION COMPLETED</b>
	X	I have completed and reviewed my responses in this section.
**	<b>NOTE:</b>	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
		<b>Section Update date</b>

**Section 4 Review:**

		<b>PRIVACY SERVICE SECTION REVIEW AND APPROVAL</b>
		The Privacy Service has not reviewed this section.

	The Privacy Service has reviewed this section. Please make the modifications described below.
X	The Privacy Service has reviewed and approved the responses in this section.
**	<b>NOTE:</b> If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit and then select "Yes" and submit again.
	<b>Section Review Date</b>

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

Angela Waddles, Privacy Officer, 501-257-2972

## 5. DATA COLLECTION:

### 5.1 Data Types and Data Uses

FIPS 199 establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization. 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 **Veteran's or Primary Subject's Personal Contact Information (name, address, telephone, etc.)**

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

The most common data types that are captured and accessed on a regular basis by authorized individuals are first and last name, middle initial, DOB, SSN, and address. This patient information falls into two classes: administrative and clinical. Clinical information is used to diagnose, prescribe treatment and follow clinically the patient through his/her health care encounters. Administrative data is used to identify the veteran (SSN), correspond to/from (name and address), and determine eligibility (patient administrative info + SSA and IRS data).

No **Other Personal Information of the Veteran or Primary Subject**

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

N/A

Yes

**Dependent Information**

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

Dependent data will be utilized to determine eligibility for VA benefits.

Yes

**Service Information**

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

Military Service Information (Branch of service, discharge date, discharge type, service connection rating, medical conditions related to military service, etc). This information is collected to assess eligibility for VA healthcare benefits, type of healthcare needed.

Yes

**Medical Information**

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

VistA-Legacy applications and meet a wide range of health care data needs. The VistA-Legacy system operates in medical centers, ambulatory and community-based clinics, nursing homes and domiciliary, and thus collects a wide range of personal medical information for clinical diagnosis, treatment, patient evaluation, and patient care. Common types of personal medical information would include lab test results, prescriptions, allergies, medical diagnoses, vital signs, etc. The information is used to treat and care for the veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of the veteran.

No

**Criminal Record Information**

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

N/A

Yes

**Guardian Information**

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

Next of kin, DNR instructions, health care proxy designation. This information is used in the notification process and as required for medical decisions.

No

**Education Information**

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

N/A

Yes

**Rehabilitation Information**

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

Treatment notes, progress notes, clinical assessments, clinical diagnosis information is collected. Used in follow-up treatment and as part of the medical history.

Yes  Other Personal Information (specify):

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.

Next-of-kin information and emergency contact information, such as name and telephone number, is collected from the veteran to use to contact other individuals in case of an emergency. In addition insurance and employment information is available on the veteran for use in billing for care.

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

None.

	<b>SECTION INCOMPLETE</b>
X	<b>SECTION COMPLETED</b>
X	I have completed and reviewed my responses in this section.
**	<b>NOTE:</b> If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	<b>Section Update Date</b>

### Section 5.1 Review:

	<b>PRIVACY SERVICE SECTION REVIEW AND APPROVAL</b>
	The Privacy Service has not reviewed this section.
	The Privacy Service has reviewed this section. Please make the modifications described below.
X	The Privacy Service has reviewed and approved the responses in this section.
**	<b>NOTE:</b> If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit and then select "Yes" and submit again.
	<b>Section Review Date</b>

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

Angela Waddles, Privacy Officer, (501) 257-2972

### 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 **Veteran Source**

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

Data used to identify the veteran, determine eligibility for care, schedule treatment and manage the provided care.

No **Public Source(s)**

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.

N/A

Yes **VA Files and Databases**

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.

For VistA-Legacy, Patient Treatment File is used to store and make inquiries of personally identifiable information about the veteran, previous clinical records, clinical information, drug information as needed to provide treatment and reimbursement.

Yes **Other Federal Agency Source(s)**

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.

IRS,SSA, DoD data used for income verification to determine if third party collection is possible. Also used in determining eligibility for care.

No **State Agency Source(s)**

*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.*

N/A

No **Local Agency Source(s)**

*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.*

N/A

No **Other Source(s)**

*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.*

N/A

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

None.

	<b>SECTION INCOMPLETE</b>
X	<b>SECTION COMPLETED</b>
X	I have completed and reviewed my responses in this section.
**	<b>NOTE:</b> If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	<b>Section Update Date</b>

**Section 5.2 Review:**

	<b>PRIVACY SERVICE SECTION REVIEW AND APPROVAL</b>
	The Privacy Service has not reviewed this section.
	The Privacy Service has reviewed this section. Please make the modifications described below.
X	The Privacy Service has reviewed and approved the responses in this section.

<b>** NOTE:</b>	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
	and then select "Yes" and submit again.
	<b>Section Review Date</b>

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

Angela Waddles, Privacy Officer, (501)257-2972

### 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.

**Web Forms:** 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.")

The web form is located at <https://www.1010EZ.med.va.gov/sec/vah/1010EZ>. This site from which this form is accessed (<http://www.va.gov/>) references the VA Privacy and Security site (<http://www.va.gov/privacy/>), as well as the VA Disclaimer site (<http://www.va.gov/disclaim.htm>) and the VA FOIA site (<http://vawww.va.gov/OIT/CIO/FOIA/default.asp>)

**Paper Forms:** 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.

VA Form 1010EZ

**Electronic File Transfer:** 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.)

N/A

**Computer Transfer Device:** 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.

N/A

<input type="checkbox"/> Yes	<b>Telephone Contact:</b>	Information is collected via telephone.
------------------------------	---------------------------	---

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

Veterans answer questions posed over phone to collect Form 1010EZ data.

<input type="checkbox"/> 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.*

N/A

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

None.

	<b>SECTION INCOMPLETE</b>
<input checked="" type="checkbox"/> X	<b>SECTION COMPLETED</b>
<input checked="" type="checkbox"/> X	I have completed and reviewed my responses in this section.
<b>** NOTE:</b>	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	<b>Section Update Date</b>

**Section 5.3 Review:**

	<b>PRIVACY SERVICE SECTION REVIEW AND APPROVAL</b>
	The Privacy Service has not reviewed this section.
	The Privacy Service has reviewed this section. Please make the modifications described below.
<input checked="" type="checkbox"/> X	The Privacy Service has reviewed and approved the responses in this section.
<b>** NOTE:</b>	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit and then select "Yes" and submit again.
	<b>Section Review Date</b>

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

Angela Waddles, Privacy Officer, (501)257-2972

**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?

Mandatory

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?

VA Form 1010EZ; VA Notice of Privacy Policies

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.)

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

A link to the VA Notice of Privacy Policies is available on our local website.

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.**

Yes **Web Forms:**

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.

Patients are allowed to download Form 1010 which contains privacy information concerning each of the data fields they are required to enter.

Yes

**Paper Forms:**

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.

Patients fill out required fields of information on Form 1010 and an explanation of privacy policy is provided.

No

**Electronic File Transfer:**

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?

There are Data Use Agreements (DUA) in place between the VA and DoD that govern the exchange of information.

No

**Computer Transfer Device:**

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?

N/A

Yes

**Telephone:**

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.

Information is obtained over a telephone interview and patients are provided with a consent form to sign

and return.

No **Other 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.*

N/A

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

None.

	<b>SECTION INCOMPLETE</b>
X	<b>SECTION COMPLETED</b>
X	I have completed and reviewed my responses in this section.
**	<b>NOTE:</b> If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	<b>Section Update Date</b>

**Section 5.4 Review:**

	<b>PRIVACY SERVICE SECTION REVIEW AND APPROVAL</b>
	The Privacy Service has not reviewed this section.
	The Privacy Service has reviewed this section. Please make the modifications described below.
X	The Privacy Service has reviewed and approved the responses in this section.
**	<b>NOTE:</b> If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit and then select "Yes" and submit again.
	<b>Section Review Date</b>

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

**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.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.

No

**Web Forms:**

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.

N/A

No

**Paper Forms:**

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.

N/A

No

**Electronic File Transfer:**

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.

N/A

No

**Computer Transfer Device:**

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.

N/A

No

**Telephone Contact Media:**

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.

N/A

No

**Other Media**

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.

N/A

**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:

Processes are in place to ensure collection of only required data. Data is collected and entered electronically with the use of *automated forms* that request only the data necessary. The use of these forms would then eliminate the collection of unnecessary data. Data collected by means of telephone are done so by completed paper forms that identify required data necessary. For example, an "Admission" form would be completed to admit a patient, therefore, only the data of these required fields would be collected.

5.6.b) How is data checked for completeness?

Data is reviewed by staff and confirmed and also compared to paper forms after data is entered electronically to ensure that all fields have been completed.

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

Administrative data is updated with each application for care. Each time a veteran is seen for an appointment, hospitalization, travel pay, etc. data is verified and updated at the time the patient presents for care or follow-up. For example, clinics verify address, next of kin and insurance information

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

New data is compared with printed form or via patient verification. The veteran brings DD214 with them and it is verified. For example, the 1010 is printed and the veteran reviews and signs that the information is accurate. For example, the VISTA system is designed to identify inconsistencies in data that is reported and provides an exception list for several applications.

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

None.

	<b>SECTION INCOMPLETE</b>
X	<b>SECTION COMPLETED</b>
X	I have completed and reviewed my responses in this section.
**	<b>NOTE:</b> If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	<b>Section Update Date</b>

**Section 5.6 Review:**

	<b>PRIVACY SERVICE SECTION REVIEW AND APPROVAL</b>
	The Privacy Service has not reviewed this section.
	The Privacy Service has reviewed this section. Please make the modifications described below.
X	The Privacy Service has reviewed and approved the responses in this section.
**	<b>NOTE:</b> If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit and then select "Yes" and submit again.
	<b>Section Review Date</b>

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

Angela Waddles, Privacy Officer, (501) 257-2972

**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.

**System Users**

**System Owner, Project Manager**

**System Administrator**

**Contractor**

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.

Most all VA contractors are required to take the privacy and cyber security training and have varied degrees of access based on their background check and level of security, as is applicable to the VA employees. Contracting support for our medical center include, but not limited to, the following: Clinical Based Outpatient Clinic contract staff provide direct patient care; transcriptions prepare documentation in support of patient care; contracted medical staff for various clinical areas provide direct patient care; Agency Nursing staff supplement staff to provide direct patient care due to increased vacancies or hard to fill positions; some contracting staff provide billing support for revenue generation, etc.

CBOC Mena	V598P-4284	HealthStar Physicians
El Dorado	V598P -4224	UAMS
Mtn Home	V598P -4323	BCLP
Hot Springs	V598P -1112	VALOR Healthcare
Medical Coding	GS-35F-0623M	TC Associates
Nurses	V598P-4451	Maxim HealthCare
	V598P-4454	NC Staffing Svcs
Admin Supp Svcs	V598P-4222	Pathfinders (JWOD)
Switchboard Svc	V598P -3669	
VISN Glucometers	V598-BP-0002	Roche Diagnostics
Radiology	V598P-1093	UAMS
Vascular Surgery	V598P -4327	
Cardio Surgery	V598P -4432	
Home Med Equipment	V598P -4387	SS Medical
Neurosurgeon	V797P-4323	CompHealth
Tri-Fab (Prosthesis)	V797P-7067A	JAS Associates

No **Internal Sharing: Veteran Organization**

*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.*

N/A

Yes **Other Veteran Organization**

*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.*

State Veterans Home for continuity of care.

No **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.*

N/A

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.*

N/A

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.*

N/A

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.*

There is certain VHA VistA patient data that is shared with DoD through the Federal/Bidirectional Health Information Exchange (FHIE/BHIE) Program under DUAs that have been in effect for several years. In addition, certain clinical information is being shared with CDC, also under an established DUA.

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.*

N/A

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

Clinical and administrative staff involved in the provision of care.

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

On a need to know basis.

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

Yes – VHA1605.1 and VHA 1605.2 A Handbooks

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

User access will be restricted.

*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)*

Processes and training materials specifically related to preventing misuse, including violation of unauthorized browsing are in place. Policies are in place restricting access to "need to know basis" and managed through menus and keys. Access is only permitted in the performance of official duties.

*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)*

No. Comment: Our contract employees follow the same security requirements such as cyber security and VA privacy training as well as a security clearance. They are given access therefore considered system users.

**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.*

Data is shared through contractor's access to the VISTA system. Information Security and Privacy policies are in place and all employees, including contract employees, are responsible for cyber security and privacy training.

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

Contract employees have access to VISTA, therefore, the data is not leaving the IT system.

Contract employees have access to VISTA.

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.

Contracts and Business Associate agreements are in place. The contracts include provisions concerning information security and privacy.

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

Access to data is obtained through access to the VISTA system and technical security controls are in place on the system. Menus and keys restrict access to only information necessary in performance of official duties. Automatic password protected screen saver ensures information is secured after 15 minutes if the computer is left unattended.

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

All individuals who obtain access to VA data must meet the security requirements such as Information Security and VA Privacy Training and must complete a security clearance before access is granted.

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

None.

	<b>SECTION INCOMPLETE</b>
X	<b>SECTION COMPLETED</b>
X	I have completed and reviewed my responses in this section.
**	<b>NOTE:</b> If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	<b>Section Update Date</b>

**Section 6.1 Review:**

	<b>PRIVACY SERVICE SECTION REVIEW AND APPROVAL</b>
	The Privacy Service has not reviewed this section.
	The Privacy Service has reviewed this section. Please make the modifications described below.
X	The Privacy Service has reviewed and approved the responses in this section.
**	<b>NOTE:</b> If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit and then select "Yes" and submit again.
	<b>Section Review Date</b>

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

Angela Waddles, Privacy Officer, (501)257-2972

**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.)

Yes	The application will provide a link that leads to their information.
No	The application will provide, via link or where data is collected, written instructions on how to access/amend their information.
Yes	The application will provide a phone number of a VA representative who will provide instructions.
Yes	The application will use other method (explain below).
NO	The application is exempt from needing to provide access.

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

Individuals may either visit the VAMC where they receive their care and begin the process or may visit the Freedom of Information Act (FOIA) Website for VA at <http://www.va.gov/oit/cio/foia/guide.asp#how> or may go through VA Forms at <http://www.va.gov/vaforms/medical/pdf/vha-10-5345-fill.pdf>. Further information regarding the VA SOR is available at [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).

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

Same as above.

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.

A notice describing the process is mailed to the patient.

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

	<b>SECTION INCOMPLETE</b>
X	<b>SECTION COMPLETED</b>
X	I have completed and reviewed my responses in this section.
**	<b>NOTE:</b> If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.

Section Update Date 11/15/07

### Section 6.2 Review:

PRIVACY SERVICE SECTION REVIEW AND APPROVAL	
	The Privacy Service has not reviewed this section.
	The Privacy Service has reviewed this section. Please make the modifications described below.
X	The Privacy Service has reviewed and approved the responses in this section.
** NOTE:	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit and then select "Yes" and submit again.
Section Review Date	

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

Angela Waddles, Privacy Officer, (501)257-2972

### 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.

**System of Records Notices may be accessed via:**

<http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm>

or

[http://vaww.va.gov/foia/err/enhanced/privacy\\_act/privacy\\_act.html](http://vaww.va.gov/foia/err/enhanced/privacy_act/privacy_act.html)

For VHA projects, VHA Handbook 1907.1 (Section 6j) and VHA Records Control Schedule 10-1 provide more general guidance.

**VHA Handbook 1907.1 may be accessed at:**

[http://www1.va.gov/vhapublications/ViewPublication.asp?pub\\_ID=434](http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=434)

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.

Start by looking at the <http://www.warms.vba.va.gov/20rsc.html>

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.

Clinical information is retained in accordance with VA Records Control Schedule 10-1. Demographic information is updated as applications for care are submitted and retained in accordance with VA Records Control Schedule 10-1. Federal law requires VA Medical Records be retained 75 years after last episode of care for continuity of patient care.

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

Electronic Final Version of Patient Medical Record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records Control Schedule 10-1, Item XLIII, 2.b. (Page 190). At the present time, VistA Imaging retains all images. We are performing a study to explore whether some images can be eliminated on an earlier schedule.

**7.c) Where are procedures documented?**

VA Handbook 6300; Record Control Schedule 10-1

**7.d) How are data retention procedures enforced?**

VA Records Control Schedule 10-1 (page 8): Records Management Responsibilities The Health Information Resources Service (HIRS) is responsible for developing policies and procedures for effective and efficient records management throughout VHA. In addition, HIRS acts as the liaison between VHA and National Archives and Records Administration (NARA) on issues pertaining to records management practices and procedures. Field records officers are responsible for records management activities at their facilities. Program officials are responsible for creating, maintaining, protecting, and disposing of records in their program area in accordance with NARA regulations and VA policy. All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures. Disposition of Records. The File Room supervisor within in Health Information Management Service (HIMS) is responsible for managing the process for pulling lists of inactive files and getting them ready for sending them to the Federal Record System. The records are accessioned for tracking by the HIMS Department.

**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.)

	<b>SECTION INCOMPLETE</b>
X	<b>SECTION COMPLETED</b>
X	I have completed and reviewed my responses in this section.
**	<b>NOTE:</b> If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	<b>Section Update</b>

**Section 7 Review:**

	<b>PRIVACY SERVICE SECTION REVIEW AND APPROVAL</b>
	The Privacy Service has not reviewed this section.
	The Privacy Service has reviewed this section. Please make the modifications described below.

X	The Privacy Service has reviewed and approved the responses in this section.
** NOTE:	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit and then select "Yes" and submit again.
	<b>Section Review Date</b>

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

Angela Waddles, Privacy Officer (501)257-2972

## 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:

Quarterly review of menus and keys is performed by the Service Management in conjunction with the Information Security Officer. Access to sensitive records is also monitored and review and any outliers are referred to management for follow-up. Separation reports are monitored to ensure staff who separate or transfer to other services have access removed and/or revised based on new duty requirements. Security Control Assessment is ongoing.

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.**

The agency is following IT security requirements as described in the FISMA. IT security is provided at the project and enterprise levels. IT security measures included the use of passwords, user authentication, physical security controls and configuration management. Enterprise level IT security includes firewalls for intrusion protection, virus protection software, and the implementation of authentication systems. Risk assessments are conducted. VistA last completed a FISMA survey in July 2003. The Office of Cyber and Information Security (OCIS) provides regular guidance on IT security issues and interpretation of rules and regulations set by legislation, policy or NIST guidelines. OCIS will serve as a point of contact for additional questions or specifics on implementation of security measures

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

At the Department level the CIO's Office of Cyber & Information Security (OCIS) is responsible for the establishment of directives, policies, & procedures which are consistent with the provisions of Federal Information Security Management Act (FISMA) as well as guidance issued by the Office of Management & Budget (OMB), the National Institute of Standards & Technology (NIST), & other requirements that VistA-Legacy is and has been subject to. In addition, OCIS administers and manages Department-wide security solutions, such as anti-virus protection, authentication, vulnerability scanning & penetration testing, & intrusion detection systems, and incident response (800-61). At the VistA-Legacy project level -The Project Manager ensures that CIO-provided security directives are integrated into the project's security plan & implemented by VA & contractor staff throughout the project Funding needs are dependent on IT security requirements identified in the system development life cycle (800-64) (i.e. risk assessments (800-30), certification and accreditation (800-37 and 800-53)), as well as identified security weaknesses that must be corrected.

**8.2.c) Explain what security risks were identified in the security risk assessment.**

There were no major security risks identified in the facility risk assessment.

**8.2.d) Explain what security controls are being used to mitigate these risks.**

Ongoing security control assessment is performed to ensure adequate security controls are in place. Actions to mitigate are documented in the SMART Plan of Action & Milestones (POA&M) database. Annual Self Assessments are also performed and mitigation is documented in SMART POA&M database.

	<b>SECTION INCOMPLETE</b>
X	<b>SECTION COMPLETED</b>
X	I have completed and reviewed my responses in this section.
**	<b>NOTE:</b> If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	<b>Section Update Date</b>

**Section 8 Review:**

	<b>PRIVACY SERVICE SECTION REVIEW AND APPROVAL</b>
--	--

	The Privacy Service has not reviewed this section.
	The Privacy Service has reviewed this section. Please make the modifications described below.
X	The Privacy Service has reviewed and approved the responses in this section.
** NOTE:	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit and then select "Yes" and submit again.
	<b>Section Review Date</b>

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

Angela Waddles, Privacy Officer (501)257-2972

**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:

**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".

**11. PIA Assessment**

11a) 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.

No choices were made regarding the system as a result of performing the PIA. Vista-Legacy is a steady state project and is governed by existing policies and procedures and governed Nationally.

11b) What auditing measures and technical safeguards are in place to prevent misuse of data?

National Directive 6500 and Handbook outlines required security controls.

11c) Availability assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization?

<input type="checkbox"/>	The potential impact is <b>high</b> if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.
<input type="checkbox"/>	The potential impact is <b>moderate</b> if the loss of availability could be expected to have

	<b>SECTION INCOMPLETE</b>
X	<b>SECTION COMPLETED</b>
X	I have completed and reviewed my responses in this section.
**	<b>NOTE:</b> If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	<b>Section Update Date</b>

**Section 11 Review:**

	<b>PRIVACY SERVICE SECTION REVIEW AND APPROVAL</b>
	The Privacy Service has not reviewed this section.
	The Privacy Service has reviewed this section. Please make the modifications described below.
X	The Privacy Service has reviewed and approved the responses in this section.
**	<b>NOTE:</b> If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit and then select "Yes" and submit again.
	<b>Section Review Date</b>

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

Angela Waddles, Privacy Officer, (501)257-2972

**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.

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

13.1) I have carefully reviewed the responses to each of the questions in this PIA R2N16 VHALIT VISTA. 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.

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

*Barbara L. B.*

B. K. Hack, Director, IT Operations, Region 2

*James P. Hall*

James P. Hall, Chief Information Officer

*Donna L. Haggard*

Donna L. Haggard, Information Security Officer

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

	<b>SECTION INCOMPLETE</b>
<input checked="" type="checkbox"/>	<b>SECTION COMPLETED</b>
<input checked="" type="checkbox"/>	I have completed and reviewed my responses in this section.
**	<b>NOTE:</b> If you are resubmitting your updates, first select "NO Value" from the dropdown and submit, and then select "Yes" and submit again.
	<b>Section Update Date</b>

**Section 13 Review:**

	<b>PRIVACY SERVICE SECTION REVIEW AND APPROVAL</b>
	The Privacy Service has not reviewed this section.

	The Privacy Service has reviewed this section. Please make the modifications described below.
X	The Privacy Service has reviewed and approved the responses in this section.
**	<b>NOTE:</b> If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
	and then select "Yes" and submit again.
	<b>Section Review Date</b>

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

Angela Waddles, Privacy Officer, (501)257-2972