Privacy Impact Assessment / {Iron Mountain VA Medical Center, Iron Mountain Michigan}

PRIVACY IMPACT ASSESSMENT 2008

INTRODUCTION:
Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.
To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person. Appendix A, "Applicable Legal and Regulatory Requirements" summarizes the applicable legal and regulatory requirements that are addressed by the PIA process.
Update regarding PIV projects: Federal Information Processing Standards Publication (FIPS PUB) 201 Personal Identity Verification (PIV) of Federal Employees and Contractors and subsequent OMB guidance explicitly require PIAs for PIV projects collecting any personal data, not just of the public.
Primary Privacy Impact Assessment objectives include:
o Ensure and promote the trust and confidence of Veterans and the general public.
o Ensure compliance with the eGov Act and other applicable privacy laws, regulations and policies, including the PIV regulations.
o Identify the risks and adverse effects of collecting, maintaining and disseminating personal information in electronic information systems.
o Evaluate and develop protections and alternative processes for handling information to mitigate potential privacy risks.
Additional important objectives include:
o Provide a mechanism for ensuring responsibility and accountability for privacy issues.
o Provide documented assurance that privacy, security and other vital data stewardship considerations are integrated into information technology systems, starting with the initial outlining of a project's objectives and data usage requirements and continuing through design, operation, maintenance and disposal.
o Ensure that decision-makers are provided the information required to make informed system design or procurement decisions, based on an understanding of privacy risk, and of options available for mitigating that risk.
o Greatly reduce the risk of needing to interrupt a program or service because privacy and other vital data stewardship considerations were not adequately addressed before the program or service was implemented.
o Promote awareness and understanding of privacy issues.
o Provide valuable documentation on the flow of personal information, and related privacy considerations and design decisions.

Completion of this PIA Form:

o Part I (Sections 1 and 2) of this form must be completed for all projects. Part I documents basic project information and establish whether a full PIA is required.

o This entire PIA Form (Parts I and II) must be completed/updated every year for all projects with information technology (IT) systems that collect, maintain, and/or disseminate "personally identifiable information" information that may be used to identify a specific person of the public, OR is a PIV project.

Important Note: While this form provides detailed instructions for completing a Privacy Impact Assessment for your project, support documents that provide additional guidance are available on the OCIS Portal (VA network access required).

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 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. Your response will be automatically limited to approximately 200 words, and should provide a basic understanding of the project, and its most essential elements. (If applicable, use of personal data is to be described in Section 3.)

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 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 rehabilitee treatment programs, 135 nursing homes, 207 readjustment counseling centers, 57 veteran benefits regional offices, and 125n ational 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:

1.2.a) Person completing this document:	
Title: Jodi Drake, Privacy Officer	
Organization: Iron Mountain VA Medical Center Iron Mountain, Michigan	
Telephone Number: 906-774-3300	
Email Address: jodi.drake @med.va.gov	
1.2.b) Project Manager:	
Title: Jodi Drake, Privacy Officer, Chief, PAS	
Organization: Iron Mountain VA Medical Center Iron Mountain, Michigan	
Telephone Number: 906-774-3300	
Email Address: jodi.drake@med.va.gov	
1.2.c) Staff Contact Person:	
Title: Jodi Drake, Privacy Officer, Chief, PAS	
Organization: Iron Mountain VA Medical Center Iron Mountain, Michigan	
Telephone Number: 906-774-3300	
Email Address: jodi.drake@med.va.gov	

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

		SECTION INCOMPLETE
	x	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 1 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)

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?

Yes

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 13 and affirm.

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

Yes 3/1/06 – PIA For Fingerprint System Clarification

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

		SECTION INCOMPLETE
	X	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 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)

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.

Providing patient health care

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

Title 5 USC, Title 38 USC, Privacy Act of 1974

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.

Iron Mountain VA Med Center VistA shows 1,400 employee records. This also includes the separated employees for the past 5 years. All employees have their records stored in the system.

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 1983 and has been fully implemented C&A since 2005.

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

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

Section 3 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)

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),
24VA19, 23VA163, 97VA105, 121VA19
(2) The name of the System of Records, and
24VA19 – Patient Medical Records-VA, 23VA163 Non-VA Fee Basis Records-VA, 97VA105 Consolidated Data Information System, 121VA19 National Patient Databases-VA
(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
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.
Medical records for patient care
4.b.4) Does the System of Records Notice require modification?
If "No" then skip to section 5, 'Data Collection'.
No

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.)

		SECTION INCOMPLETE
	X	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 4 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)

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."

y/n?	Veteran's or Primary Subject's Personal Contact Information (name, address, telephone, etc.)

Yes

Specifically identify the personal information collected, and describe the intended use of the information.
Name, gender, date of birth, marital status, race, ethnicity, religious preference, social security number, address, phone number, parents names
Used for patient registration and patient care

y/n?	Other Personal Information of the Veteran or Primary Subject

Yes

Specifically identify the personal information collected, and describe the intended use of the information.
Medical information in CPRS – used for patient care

y/n?	Dependent Information

Yes

Specifically identify the personal information collected, and describe the intended use of the information.
Name, address, phone number of spouse/children of veterans who have applied for health care services, used in determining benefits, emergency contacts, and next of kin information.

y/n?	**Service Information**

Yes

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

Branch and dates of service, type of discharge, veterans military history

Used to verify status for VA medical care and for patient treatment

y/n?	**Medical Information**

Yes

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

All medical information in VISTA/CPRS – used for patient care

y/n?	**Criminal Record Information**

No

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

y/n?	**Guardian Information**

Yes

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

Name, address, phone number of guardians for incapacitated patients.

Used for communication purposes and patient care, guardians are used to assist with communication with patients.

y/n?	**Education Information**

Yes

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

Patient educational information is made available to clinicians treating patients to help understand their medical conditions. Patients are educated on their conditions as well.

y/n?	**Rehabilitation Information**

Yes

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

Rehabilitation information is collected for patients being treated in special programs including strokes, cardiac conditions, head injuries, spinal cord injuries, blindness, alcohol and drugs, PTSD, amputees, functional dependence.

Used for patient care

y/n?	**Other Personal Information (specify):**

No

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.

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

		SECTION INCOMPLETE
	X	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 5.1 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)

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.

y/n?	**Veteran Source**

Yes

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

Collected for patient registration and health care.

y/n?	**Public Source(s)**

No

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.

y/n?	**VA Files and Databases**

Yes

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.

VISTA files – used for patient care and clinical decision-making.

y/n?	**Other Federal Agency Source(s)**

Yes

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.

Dept. of Defense clinical data – used for patient care

y/n?	**State Agency Source(s)**

No

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.

y/n?	**Local Agency Source(s)**

No

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.

y/n?	**Other Source(s)**

No

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.)

		SECTION INCOMPLETE
	X	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 5.2 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)

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.

y/n?	**Web Forms:**	Information collected on Web Forms and sent electronically over the Internet to project systems.

No

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.")

y/n?	**Paper Forms:**	Information collected on Paper Forms and submitted personally, submitted via Postal Mail and/or submitted via Fax Machine.

Yes

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

Form letter used to collect insurance information

y/n?	**Electronic File Transfer:**	Information stored on one computer/system (not entered via a Web Form) and transferred electronically to project IT systems.

Yes

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.)

Patients and their caregivers enter vital measurements and blood glucose levels into Home telehealth devices for entry into VISTA system.

Used for patient care. Used for health care to veterans and administration of employee information for pay, employee health and personnel actions.

y/n?	**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.

No

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

y/n?	**Telephone Contact:**	Information is collected via telephone.

Yes

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

Telephone triage by Nursing – collects symptoms and information for patient care.

Utilization Review Nurses – precertifications from insurance companies.

y/n?	**Other Collection Method:**	Information is collected through a method other that those listed above.

No

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.)

		SECTION INCOMPLETE
	X	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 5.3 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)

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?

Notices are sent by National Health Eligibity Center upon patient enrollment.

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.)

X	**Not applicable**
	Privacy notice is provided on each page of the application.
	A link to the VA Website Privacy Policy is provided.
	Proximity and Timing: the notice is provided at the time and point of data collection.
	Purpose: notice describes the principal purpose(s) for which the information will be used.
	Authority: notice specifies the legal authority that allows the information to be collected.
	Conditions: notice specifies if providing information is voluntary, and effects, if any, of not providing it.
	Disclosures: notice specifies routine use(s) that may be made of the information.

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

N/A

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.

y/n?	**Web Forms:**

No

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.

y/n?	**Paper Forms:**

Yes

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.

Form letter is sent to patient to collect insurance information. Form letter notes what information is being collected. Privacy notice will be added to the form letter.

y/n?	**Electronic File Transfer:**

Yes

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?

Patients and caregivers are educated on entering information into telehealth devices for entry into VISTA system. The are educated on privacy and proper entry procedures.

y/n?	**Computer Transfer Device:**

No

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?

y/n?	**Telephone:**

Yes

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 contacted by telephone and educated on the purpose for the telephone contact. They are educated verbally that the telephone call is private.

y/n?	**Other Method:**

No

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.)

		SECTION INCOMPLETE
	X	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 5.4 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)

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.

y/n?	**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.

y/n?	**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.

y/n?	**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.

y/n?	**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.

y/n?	**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.

y/n?	**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.

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

		SECTION INCOMPLETE
	X	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 5.5 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)

5.6 Data Quality

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

Data is collected electronically based on the automation of VA forms and clinical procedures. User access is limited therefore their ability to collect data is also limited. Access is limited by menu and key assignments. Access is based on job function; menus and keys are requested by service supervisors.

5.6.b) How is data checked for completeness?

Each service has their own internal policies and procedures for checking data input for completeness. Data is reviewed by supervisors and staff and compared to paper forms where available. In many cases there are internal checks within the software i.e. checking data entered on previous dates against current data.

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

Clinical data is not removed from the Vista system. Administrative data is updated with each application for care. Patient data is updated at each appointment. All data within Vista is time-stamped i.e. any changes are clearly identified by date and who made the change.

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

New data is compared with printed form (if available), via patient verification, or by comparison to previously entered data.

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

		SECTION INCOMPLETE
	X	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 5.6 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)

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.

y/n?	**System Users**

Yes

y/n?	**System Owner, Project Manager**

Yes

y/n?	System Administrator

Yes

y/n?	Contractor

Yes

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.

EPRP reviews done by VHA contractors using CPRS.
Transcription vendor types and uploads reports into VISTA.

y/n?	Internal Sharing: Veteran Organization

No

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.

y/n?	Other Veteran Organization

Yes

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.

VBA data used thru CAPRI. Information relating to benefits shared with Veterans Benefits Affairs offices.

y/n?	Other Federal Government Agency

Yes

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.

Dept. of Defense bi-directional health exchange – used for patient care, health care information.

y/n?	State Government Agency

Yes

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.

State Cancer Registry – cancer diagnosis, staging, and follow-up
Used for patient care and statistics.

y/n?	Local Government Agency

No

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.

y/n?	**Other Project/ System**

No

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.

y/n?	**Other User(s)**

No

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:

Clinical and administrative staff involved in the provision of care.

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

User access is limited through the assignment of menus and keys. Access is based on job function. Menus and keys are requested/approved by service supervisors.

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

Yes – VHA1605.1 and VHA 1605.2 VA 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 through the limited assignment of menus and key. Access is based on job function. Menus and keys are requested/approved by service supervisors.

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 currently being developed and projected to be available next FY. Those who share information are educated on privacy and protection of data, and appropriate use.

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. Only authenticated system users have access to Vista data.
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.
Those who share information are educated on privacy rules and regulations. Information is monitored for privacy and use.
6.1.h) Identify who is responsible, once personal information leaves your project's IT system(s), for ensuring that the information is protected.
6.1.i) Describe how personal information that is shared is transmitted or disclosed.
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.
6.1.k) How is the shared information secured by the recipient?
6.1.l) What type of training is required for users from agencies outside VA prior to receiving access to the information?
ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

		SECTION INCOMPLETE
	X	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 6.1 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)

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.)

	The application will provide a link that leads to their information.
	The application will provide, via link or where data is collected, written instructions on how to access/amend their information.
	The application will provide a phone number of a VA representative who will provide instructions.
X	**The application will use other method (explain below).**
	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?

Written request and authorization to Release of Information Unit using VAF 10-5345a.

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

Written request by veteran to Privacy Officer identifying any inaccurate information and describing the preferred remedy desired. Request is reviewed and a determination made to grant or deny the individual's request. The determination is communicated to the individual. If the request is granted, the record is amended.

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

If the request is denied, the individual may appeal to VA General Counsel.

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

Notice of Access & Amendment is published in System of Records notice for 24VA19 Patient Medical Record – VA.

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

		SECTION INCOMPLETE
	X	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

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)

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
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
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/20rcs.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.
75 years after patient's last episode of care. Specified in 24VA19 Patient Medical Records-VA
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, (hard-drives) must be disposed of by degaussing rendering them inoperable via contract vendor Intelligent Decision
7.c) Where are procedures documented?
VHA Record Control Schedule 10-1
7.d) How are data retention procedures enforced?
No records are disposed/destroyed without approval of the Record Control Manager. All records are disposed of in accordance with VA Policy and disposition authority.
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.)

		SECTION INCOMPLETE
	X	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 7 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)

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:

The Information Security Officer has security menu and options for Auditing. System Administrators regularly monitor performance and availability. Certification and Accreditation is ongoing. Changes to the system are tested and evaluated through a national alpha and beta testing system prior to release to local facility and implementation.

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

Yes, **Computer Room** is located on center 5th floor. Building, is of Brick masonry construction with embedded windows. Two (2) doors are secured via a card key system, The facility is equipped with an intrusion detection alarm system that is monitored by the local VA police. The computer room has two entrance. Card key entrance into offices hallway which leads to main computer room raised floor, recessed ceiling environment. Each door has a card key system with access level that is in operation twenty four (24) hours a day, seven (7) days a week. Main entrance to office area is locked need key card to enter or press buzzer for IRM staff to allow

entry.
Fire Detection and Suppression: Fire detection system consists of heat detectors and ionization-type smoke detectors located above ceiling. The fire alarm system is also monitored by the local VA Police. Sprinkler heads located in ceiling.
Energy Management: Liebert air conditioning units that compensate for the generated heat load, which varies across seasons, environmentally control the data center.
Electrical power is provided by redundant feeds originating in separate commercial electric power substations. Two Emerson Electric automatic transfer switches and two Liebert Uninterruptible Power System (UPS) provide critical electrical power.

Off Site Data Storage: Data center backsup all data media storage on a daily basis. The data storage media are then transported to VA Hines Medical Center. VA Hines Storage Data Center meets all Government requirements for an off-site storage facility.

Hot-Site for Disaster Recovery: Jesse Brown VA Med Center has a contract with VA Hines for hot site support. In the event of a total or partial disaster and the decision is made to activate the hot-site, a designated team will travel to the hot site to operate the facility in place of the Jesse Brown VA Med Center Chicago, Illinois VISN 12, Region 2.

Yes. Access to the main computer system requires individuals to sign in with Name, Date, Time, Purpose, Time of Exit. Contractors and vendors are escorted.

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 intusion protection, virus protection software, and the implementation of authentication systems. Risk assessments are conducted. VistA last completed a FISMA survey in Jul 2003. The Office of Cyber and Information Security 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.

VistA Imaging has completed the C&A process successfully. The Vista Imaging Security Plan identifies how the requirements and procedures will be address. (SSP). NIST SP 800-53 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.

REMOVED (SENSITIVE INFORMATION)

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

REMOVED (SENSITIVE INFORMATION)

		SECTION INCOMPLETE
	X	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 8 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)

Jodi Drake, Chief, PAS Ext. 32601

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.*

		SECTION INCOMPLETE
	X	**SECTION COMPLETE**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 9 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)

Jodi L Drake, Chief, PAS, Privacy Officer 906-774-3300, Ext. 32601

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.)

		SECTION INCOMPLETE
	X	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 10 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)

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.			
None			
11b) What auditing measures and technical safeguards are in place to prevent misuse of data?			
Random audits of users.			
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?			
X		**The potential impact is <u>high</u> if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.**	
	y/n?	**The potential impact is <u>moderate</u> if the loss of availability could be expected to have a serious adverse effect on operations, assets, or individuals.**	
	y/n?	**The potential impact is <u>low</u> if the loss of availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.**	
11d) Integrity assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?			
X	y/n?	**The potential impact is <u>high</u> if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.**	
	y/n?	**The potential impact is <u>moderate</u> if the loss of integrity could be expected to have a serious adverse effect on operations, assets, or individuals.**	
	y/n?	**The potential impact is <u>low</u> if the loss of integrity could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.**	
11e) Confidentiality assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization?			
X	y/n?	**The potential impact is <u>high</u> if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.**	
	y/n?	**The potential impact is <u>moderate</u> if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets, or individuals.**	
	y/n?	**The potential impact is <u>low</u> if the loss of confidentiality could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.**	
11f) What was the highest impact from questions 11c, 11d, and 11e?			
Moderate			
11g) What controls are being considered for this impact level?			
Controls implemented are at the requirements for a High impact level system. NIST 800-53, for moderate risk.			
ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)			

		SECTION INCOMPLETE
	X	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 11 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)

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 assessment9. 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.)

		SECTION INCOMPLETE
	X	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 12 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)

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.

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

Jodi L Drake, Chief, PAS, Privacy Officer 07/18/2008

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

		SECTION INCOMPLETE
	X	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 13 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)

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.

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

Jodi L. Drake, Chief, Patient Administrative Service, Privacy Officer 07/18/2008

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

Jodi L Drake

		SECTION INCOMPLETE
	X	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	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

Section 13 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)