

**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:

REGION 1 > VHA > VISN 20 > Spokane VAMC > VISTA KERNEL

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.)*

Each Veterans Affairs (VA) medical center uses VistA (formerly DHCP, Decentralized Hospital Computer Program), an integrated hospital information system. DHCP was an M-based internally developed portfolio and VistA encompasses DHCP and a variety of other clinical and administrative applications, some on single-use platforms. VistA operates on a Virtual Memory System (VMS)/Cache platform.

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: Rob VanBommel/Ken Klein/Mark Brown**

**Title: Privacy Officer/ISO/CIO**

**Organization: DVA**

**Telephone Number: 509-434-7500**

<b>Email Address: Robert.vanbommel@va.gov</b>	
<b>1.2.b) Project Manager: Robert Van Bommel</b>	
<b>Title: Privacy Officer</b>	
<b>Organization: DVA</b>	
<b>Telephone Number: 509-434-7500</b>	
<b>Email Address: Robert.vanbommel@va.gov</b>	
<b>1.2.c) Staff Contact Person: Bruce Cook</b>	
<b>Title: IT Specialist</b>	
<b>Organization: DVA</b>	
<b>Telephone Number: 509-434-7430</b>	
<b>Email Address: bruce.cook@va.gov</b>	

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

		<b>SECTION INCOMPLETE</b>
	x	<b>SECTION COMPLETED</b>
		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: 05/27/08</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.
	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 06/02/08</b>
--	--	-------------------------------------

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?

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 13 and affirm.**

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

Yes

2.d) Have 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>
	x	<b>SECTION COMPLETED</b>
		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 06/02/08</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.
	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 06/02/08</b>

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 Care and Employee Management

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

SOR 79 VA 19, Privacy Act, 5 U.S.C. 552a(e)(4)

*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.*

Between 50,000-200,000 patients and 3,000 to 8,000 employees.

*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.*

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.*

Between 20 to 25 years ago.

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

No

		<b>SECTION INCOMPLETE</b>
	X	<b>SECTION COMPLETED</b>
		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 06/02/08</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.
	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 06/02/08</b>

*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),

SYSTEM #	SYSTEM NAME	PROGRAM OFFICE/SYSTEM MANAGER
79VA19	Veterans Health Information System and Technology Architecture (VISTA)-VA	Office of Information (19)

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

SYSTEM #	SYSTEM NAME	PROGRAM OFFICE/SYSTEM MANAGER
79VA19	Veterans Health Information System and Technology Architecture (VISTA)-VA	Office of Information (19)

(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/systemofRecords.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?

Yes

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

N/A

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.

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.

Explanation:

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

		<b>SECTION INCOMPLETE</b>
	X	<b>SECTION COMPLETED</b>
		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 06/02/08</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 06/02/08</b>

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."*

5.1.a.1

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

Yes

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

Name, SSN, DOB, Age, Address, Telephone numbers, Geographic Location.

The intended use of this information is to appropriately identify the patient and accurately link patient records under VA systems as appropriate to provide for accurate clinical decision making and continuity of care.

5.1.b.1

y/n?	<b>Other Personal Information of the Veteran or Primary Subject</b>
------	---

Yes

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

Next of Kin and Emergency Contact information; names, addresses, phone numbers.

Used for notification in case of emergency.

5.1.c.1

y/n?	<b>Dependent Information</b>
------	------------------------------

NO

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

5.1.d.1

y/n?	<b>Service Information</b>
------	----------------------------

Yes

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

information.

Military branch, rank, discharge information, and dates of service - as described on the official DD-214.

**Service Information for both benefits and Eligibility needs**

5.1.e.1

<input type="checkbox"/> y/n?	<b>Medical Information</b>
-------------------------------	----------------------------

Yes

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

Diagnosis, medical history, current problem list, prescriptions, surgeries and family history.

All medical information is to provide care to veterans. The clinicians have the responsibility to distinguish between relevant and irrelevant information that relates to the care of the veteran.

5.1.f.1

<input type="checkbox"/> y/n?	<b>Criminal Record Information</b>
-------------------------------	------------------------------------

Yes

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

Name, SSN, DOB, Address, Telephone numbers, Geographic location.

Required by Federal statute to identify wanted felons.

5.1.g.1

<input type="checkbox"/> y/n?	<b>Guardian Information</b>
-------------------------------	-----------------------------

Yes, where applicable

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

Name, address, Telephone numbers, Geographic location

Guardian information on those veterans where necessary for identification and benefit disbursement, as well as medical decision-making factors.

5.1.h.1

<input type="checkbox"/> y/n?	<b>Education Information</b>
-------------------------------	------------------------------

NO

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

5.1.j.1

<input type="checkbox"/> y/n?	<b>Rehabilitation Information</b>
-------------------------------	-----------------------------------

Yes

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

information.

Level of disability requiring rehabilitation and outside facility providing said rehabilitation if applicable.

Rehabilitation information collected is used to determine the patient historical progress and used to assist in appropriate treatment care planning.

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.

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>
		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: 04/22/08</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 06/02/08</b>

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.

To provide health care and benefits

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

N/A

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

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 and VistA imaging.

Information collected is used to provide for the continuity of care of our Veterans

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.*

SSA - financial data for benefits and death notifications

DOD - Military Data Information Systems (MDIS) provides veterans military and health records for eligibility and treatment

VA/DOD Polytrauma information to better treat traumatic injuries from OIF/OEF

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.*

N/A

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

N/A

*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

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.)

<input type="checkbox"/>	<b>SECTION INCOMPLETE</b>
<input checked="" type="checkbox"/>	<b>SECTION COMPLETED</b>
<input 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 06/02/08</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 06/02/08</b>

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?	<b>Web Forms:</b>	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?	<b>Paper Forms:</b>	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.

VA Form 1010, VA Form 1010EZ, DD 214, VA Form 10-7131

<input type="checkbox"/> y/n?	<b>Electronic File Transfer:</b>	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.)

PDX transmissions, Pharmacy for CMOP - these are vista system to vista systems ftp transfers

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

Yes

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

Outside medical records are sometimes brought in on CD-ROM or other media as well as paper, and the data then transferred into our system.

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

Yes

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

Identity is verified by asking the Veteran or authorized representative specific questions that can be verified by using information in the VA record.  
Part of the data verification process involves our Health Plan Management (i.e. the Business Office) calling to verify on an annual or bi-annual basis the demographic, financial, insurance, and other such billing information from the patient.

<input type="checkbox"/> y/n?	<b>Other Collection Method:</b>	Information is collected through a method other than 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.

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>
		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 04/02/2008</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.
	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 04/02/2008</b>

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?

Both

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?

If research, via a consent form. If general VA collection, via Notice of Privacy Practices which is provided to the patient upon enrollment of care or upon request. The notice can also be viewed online. VA Form 1010EZ; VA Notice of Privacy Policies

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

The data collection for this system is both new and 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.)

**PII is not collected online for routine patient care.**

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

This issue is under review and links to all web sites in the future will include a link to the VA Privacy Policy.

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:**

**Not Used**

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 in the near future may be allowed to download Form 1010 which contains privacy information concerning each of the data fields they are required to enter.

y/n?

**Paper Forms:**

Consent forms or waiver of authorization

*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

The consent form contains information on the project and confidentiality.

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?*

The consent form or waiver of authorization are fairly complete including all of the items in the below checklist.

The consent form contains information on the project and confidentiality.

y/n?

**Computer Transfer Device:**

Yes, Consent forms should be used or waiver of authorization

*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?*

The consent form or waiver of authorization are fairly complete including all of the items in the below checklist.

The consent form contains information on the project and confidentiality.

y/n?

**Telephone:**

Yes, Consent forms should be used or waiver of authorization

*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.*

The consent form or waiver of authorization are fairly complete including all of the items in the below checklist.

The consent form contains information on the project and confidentiality.

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.

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>
		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 06/02/08</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 06/02/08</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.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.)*

		<b>SECTION INCOMPLETE</b>
	X	<b>SECTION COMPLETED</b>
		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 06/02/08</b>

**Section 5.5 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 06/02/08</b>
<i>PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)</i>		

<b>5.6 Data Quality</b>	
<i>5.6.a) Explain how collected data are limited to required elements:</i>	
For Vista, the number and type of fields in the data files limited the data collection to just the required elements	
<i>5.6.b) How is data checked for completeness?</i>	
Must meet field parameters to be able to enter. However for free text fields, the person gathering and entering the data must check themselves manually. There is no automatic way to check the data's completeness unless you know what answer SHOULD be.	
<i>5.6.c) What steps or procedures are taken to ensure the data are current and not out of date?</i>	
Some fields are computed, for example: A date of birth is entered, so the age is computed by the program so that it is dynamic as age is not a static piece of information. Generally computed fields are things that do have a dynamic change component. Medical data is entered and reviewed by the caregiver who collects it and is cross-checked by eligibility and Health Plan Management (i.e. the Business Office). Medical information such as the Patient Problem List is checked and validated at each patient visit by that caregiver. Demographic, billing, and other such administrative data is collected by the Health Plan Management staff who have an annual or bi-annual responsibility to confirm that information is up-to-date.	
<i>5.6.d) How is new data verified for relevance, authenticity and accuracy?</i>	
Person taking the information is to validate it with the veteran or the veteran's guardian in the case of administrative data. Medical data is validated by the expertise of the clinicians.	
<i>ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)</i>	
	<b>SECTION INCOMPLETE</b>

	X	<b>SECTION COMPLETED</b>
		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 06/02/08</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 06/02/08</b>

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.*

Generally speaking, the contracts are for equipment and software maintenance and the access is granted on that basis. Some contractors are functioning as staff members, such as our PC technicians and computer help desk, they are granted access necessary to perform their job functions.

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**

No

*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.*

y/n? **Other Federal Government Agency**

No

*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.*

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 Veterans Home personnel are granted access under contract for read-only purposes to manage patient care.

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**

Yes

*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.*

Fairchild AFB is part of the DOD/VA sharing Project

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:**

VA workforce members.

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

Functional categories.

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

Yes, see IM-02 and ISS-01

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

No, access limited to just that to perform job duties.

**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)**

Active directory to limit permissions. Audits and reviews of access to confirm it meets current job 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)

Yes

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

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

A DUA or DTA is utilized to protect Veterans privacy. **Error! Not a valid link.**

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

The DUA or BAA identifies the responsible entity

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

Via encrypted electronic transfer, secure abstracting and paper transfer via secure mail such as Fed Ex.

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.

All current data sharing projects are covered under an MOU, BAA, DUA or Contract.

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

Electronic information is required to reside in an encrypted file or db. Paper files are expected to be secured in locked areas.

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

All users are required to complete VA's Privacy Training.

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

NONE

		<b>SECTION INCOMPLETE</b>
	X	<b>SECTION COMPLETED</b>
		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 05/14/08</b>

**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.
**	<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 06/02/08</b>

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.)

Local Policy **NM 136-12-07** via request or by contacting ROI clerk in the Medical Records Department either in person, phone or mail. Many Veterans also contact the Privacy Officer as identified by posters placed throughout the facility.

X	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.
X	The application will provide a phone number of a VA representative who will provide instructions.
	The application will use other method (explain below).
	The application is exempt from needing to provide access.

The information is in the VistA system and on our Intranet Page for staff. Non-VA users can access via the Privacy Website that all Veterans have access to.

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



L:\Iss\Admin\Sweden Policies\_Directives\_Pr

Local Policy NM 136-12-07. VA Directive 1605.1 **Error! Not a valid link.**

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

Local Policy NM 136-12-07. VA Directive 1605.1. A Veteran can request information be changed in his or her medical record by requesting an amendment to the record in writing. A provider can change information in a Veteran's record by placing an addendum in the record.

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

Local Policy NM 136-12-07. VA Directive 1605.1. Redress is always provided via appeal through the Regional counsel's Office

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

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>
		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 05/14/08</b>

**Section 6.2 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 06/02/08</b>

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.
<b>System of Records Notices may be accessed via:</b>
<a href="http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm">http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm</a>
or
<a href="http://vaww.va.gov/foia/err/enhanced/privacy_act/privacy_act.html">http://vaww.va.gov/foia/err/enhanced/privacy_act/privacy_act.html</a>
For VHA projects, VHA Handbook 1907.1 (Section 6j) and VHA Records Control Schedule 10-1 provide more general guidance.
<b>VHA Handbook 1907.1 may be accessed at:</b>
<a href="http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1469">http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1469</a>
For VBA projects, Records Control Schedule (RCS) VB-1 provides more general guidance. VBA Records Control Schedule (RCS) VB-1 may be accessed via the URL listed below.
Start by looking at the <a href="http://www.warms.vba.va.gov/20rcs.html">http://www.warms.vba.va.gov/20rcs.html</a>

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

75 years - Please see this National Document which Spokane VAMC follows: RCS 10-1 is located at the following hyperlink: <http://www1.va.gov/vhapublications/RCS10/rcs10-1.pdf>

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

Based on national directive there is no current authority to destroy

7.c) Where are procedures documented?

See above

7.d) How are data retention procedures enforced?

Audit

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

NO

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

NONE

		<b>SECTION INCOMPLETE</b>
	x	<b>SECTION COMPLETED</b>
		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 05/27/08</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.
**	<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 06/02/08</b>

*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.):*

X		The project is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured.
X		The project has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.
X		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 ECSIP Security Operation Center monitors DOS, virus, worm, and all other types of vulnerabilities at a national level 24/7. The local site cannot describe what the national team is

doing; we are not involved, please contact them.

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

Yes, as far as the local site is aware as this is managed at a National level.

## 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. And located on the C&A site is the VistA System Security Plan that contains all security controls; the template was provided and reviewed by VACO OI&T and outside auditors as required by the VA Certification and Accreditation Program. As all this is managed at the national level, the local facility responds to the requirements from VACO. The re-certification of the system is also at the national level. If you need more than this to explain how this meets IT security requirements, contact National. This IS an ongoing process and all security controls are governed by VA 6500 for all sites in the VA network.

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.

And system is certified and accredited. Please see the National C&A project description for more details. This is an ongoing process NOT just an every three year thing. VistA resides at the Regional level and Security controls are also there. The system does not reside at the local facility but rather at the national level.

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

There were no vulnerabilities identified during the risk assessment conducted in 2007. If, during the next assessment, vulnerabilities are identified we will upload to the C&A site and do a POA&M for them and mitigate risks in a timely manner.

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

N/A as none were identified.

		<b>SECTION INCOMPLETE</b>
	X	<b>SECTION COMPLETED</b>
		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 06/02/08</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.
**	<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 06/02/08</b>

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

**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.

		<b>SECTION INCOMPLETE</b>
	X	<b>SECTION COMPLETE</b>
		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 06/02/08</b>

### Section 9 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 06/02/08</b>

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

### 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.)

		<b>SECTION INCOMPLETE</b>
	X	<b>SECTION COMPLETED</b>
		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 06/02/08</b>

**Section 10 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 06/02/08</b>

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.

No choices were made during the performance of this PIA. Unable to do so based on this document.

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

See System Security Plan above.

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?

Y	y/n?	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.
	y/n?	The potential impact is <b>moderate</b> 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 <b>low</b> 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?

Y	y/n?	The potential impact is <b>high</b> 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 <b>moderate</b> 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 <b>low</b> 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?

Y	y/n?	The potential impact is <b>high</b> 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 <b>moderate</b> 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 <b>low</b> 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?

Confidentiality & Availability or HIGH

11g) What controls are being considered for this impact level?

VA handbook 6500 security control baselines defined in NIST Special Publication 800-53, *Security Controls for Federal Information Systems for HIGH..*

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


		<b>SECTION INCOMPLETE</b>
	X	<b>SECTION COMPLETED</b>
		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 05/14/08</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 06/02/08</b>

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 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?

Yes

12.b) If yes, specify:

Contains VA and local policies on release and safe guarding of patient information.

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

		<b>SECTION INCOMPLETE</b>
	X	<b>SECTION COMPLETED</b>
		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 06/02/08</b>

**Section 12 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 06/02/08</b>

*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)

This Signature page SCANNED to PDF format, uploaded to C&A site, per privacy service requirement.

\_\_\_\_\_  
Mark Brown, CIO

\_\_\_\_\_  
Date

\*\*\*\*\*signed/scanned/uploaded in PDF Format to C&A Site\*\*\*\*\*

\_\_\_\_\_  
Mark Brown, CIO

\_\_\_\_\_  
Signature/Date

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

		<b>SECTION INCOMPLETE</b>
	X	<b>SECTION COMPLETED</b>
		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 06/02/08</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 06/02/08</b>

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

Robert VanBommel, Privacy Officer

