

Privacy Impact Assessment – FY 2008 IT (VistA)

PIA SECTIONS 1 - 8

Part I. Project Identification

1. PROJECT IDENTIFICATION: PRIVACY IMPACT ASSESSMENT 2007 FY 2008

INTRODUCTION:

The E-Government Act of 2002 (eGov) requires that Federal agencies conduct a privacy impact assessment (PIA) for projects with information technology (IT) systems that collect, maintain, and/or disseminate individually identifiable information of the public, not including information on Federal employees or others working for the agency (e.g., contractors, interns, etc.). This "personally identifiable information" (PII) is information that can be used to identify a specific person.

A privacy impact assessment is an analysis that seeks to identify and mitigate the privacy and security risks associated with the use of personal information by a project, system or practice. A privacy impact assessment provides a framework for ensuring that privacy, security and other vital data stewardship issues are identified, addressed and incorporated into the conception, design, operation, redesign, maintenance, and disposal of electronic information systems. These PIAs also form the basis for VA's privacy reviews of all privacy-protected data as mandated by VA Directive 6502 Privacy Program, section 3.d.(7). ALL PROJECTS MAINTAINING PERSONAL INFORMATION OF THE PUBLIC IN IT SYSTEMS MUST COMPLETE A PIA EVERY YEAR.

For the goal of encouraging eGov, these PIAs will:

- o Ensure and promote the trust and confidence of veterans and the general public in VA's stewardship of their personal information.
- 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 privacy risks.
- 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, redesign and maintenance.
- 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.
- o Ensure compliance with applicable privacy law and regulations, as well as accepted privacy policy.

1.1) Project Basic Information:

1.1.a) OMB Unique Project Identifier: 029-00-01-11-01-180-00

1.1b) Brief Description of Project

VistA system provides VA patients with an integrated inpatient and outpatient electronic health record. It also provides the administrative tools to deliver veterans the best quality medical care.

It has grown to become the largest and best electronic medical record system in the world. VistA is growing more difficult to support due to: technological age, product maintenance costs and integration difficulties associated with mainstream software languages, tools, and processes. VistA software is written in MUMPS, a 20 year old technology. Improvements are also needed such as data storage in veteran-centric format and standard data that is shareable across the

enterprise to provide advanced clinical decision support. VistA stores data in a facility-centric format rather than the more useful veteran-centric format and the data is not standardized among facilities thus making decision support very difficult.

The VistA-Application Development (V-AD) replaces the existing VistA-Legacy by utilizing the framework provided by the VistA-Foundations Modernization (V-FM) program. V-FM generally consists of the hardware, software, and operating systems that enable the full function of the VistA business applications as designed. V-FM focuses on implementing standards for data representation, terminology and information exchange. V-AD consists of the enhancement and development activities that support the movement of the existing MUMPS-based applications into the HealthVet architecture, data structures, and desired capabilities. The existing VistA-Legacy applications will be re-hosted, replaced, re-engineered, or retired over the course of the lifecycle of this project. V-AD will utilize a framework that allows for alternative technical solutions and vendor competitiveness that will both decrease cost from competitive pricing and increase the functionality delivered. For VHA to continue to provide cost effective, world class medical care, the transition to a modern, open sourced IT system is a necessity. The use of the new architecture will greatly improve system affordability, scalability, interoperability, maintainability, and performance. V-AD provides a means to deliver reliable, accessible, timely health care information in an efficient manner, meeting a stated objective in VA's strategic goal of Honor and Serve Veterans in Life and an Enabling strategic objective of implementing a One VA information technology framework that supports the integration of information across business lines, reliably, accurately, and securely. These provisions satisfies the PMA E-Gov initiative, that calls for the federal government to champion citizen-centered electronic processes that result in a major improvement in the government's value to the citizen.

VistA provides a means to deliver reliable, accessible, timely health care information in an efficient manner, meeting a stated objective in VA's strategic goal of Honor and Serve Veterans in Life and an enabling strategic objective of implementing a One VA information technology framework that supports the integration of information across business lines, reliably, accurately, and securely.

1.2) Contact Information:

1.B) Contact Information:	
1.B.1) Person completing this document:	
Name:	Cheryl Johnson
Organization:	VA North Texas HCS
Telephone Number:	(214) 857-1432
Email Address:	Cheryl.Johnson3@va.gov
1.B.2) Project Manager:	
Name:	Lucy Rogers

Telephone Number:	(214) 857-2044
Email Address:	Lucy.Rogers@va.gov
1.B.3) Staff Contact Person:	Brett T. Coleman
Title:	IT Specialist
Organization:	VA North Texas HCS
Telephone Number:	(214) 857-2072

2. DETERMINATION OF PIA REQUIREMENTS:

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

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

NO

3. PROJECT DESCRIPTION:

The One-VA Registration and Eligibility program – Will provide reliable and consistent information to NTXHCS lines of business for benefit, health, contact and identification information to our veteran population. It will reduce the need to duplicate Department of Defense (DoD), Defense Manpower Data Center (DMDC) data and will establish a veteran information standard to share information between NTXHCS and DOD.

The One-VA Contact Management program – Will replace the numerous veteran registration processes currently in place, with a single process, that permits veterans to register and apply for benefits only once and in any location.

The EPP project collects information to provide VA a centralized, auditable database of all privacy complaints and violations and to comply with Health Insurance Portability and Accountability Act (HIPAA) regulations. This system is called the Privacy Violation Tracking System (PVTs) in place here since 3/07.

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

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

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

| 1,000,000 - 9,999,999 |

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

| 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.

| 24 years |

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?

| Yes |

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

Yes

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

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

Vista Records **SOR- 79VA19**

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

The Vista System

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

htm http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf

4.c) If a System of Records identifier has been assigned, then provide the name of the applicable SOR.

Computerized Patient Record System (CPRS)

4. d.) Have you read and will the application comply with all data management practices in the SOR?

Yes

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

http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf

4. e.) Is this a new System of Records or an existing SOR?

Existing

4. f.) If existing, does the System of Records require modification?

No

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

PIA SECTION 5

5. DATA COLLECTION:

5.1 Data Types and Data Uses

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

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

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

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

Yes **Veteran's or Primary Subject's Personal Contact Information (name, address, telephone, etc.)**

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

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

Yes **Other Personal Information of the Veteran or Primary Subject**

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

Collecting information such as Mother's maiden name, Date and Place of Birth, Gender, Race, Religion, Marital Status, Employment, Health Insurance, and Financial information which will be used for eligibility and patients' medical treatment.

If the complainant provides the Privacy Officer with any other personal information, it may be used for the complaint resolution.

Yes **Dependent Information**

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

Next of Kin, Spouse and children's personal information is collected, to include name and SSN. To identify individuals and to communicate with individuals about their health benefits. To determine eligibility and enroll veterans for health care services.

Yes **Service Information**

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

Branch of Service, Entry Date, Discharge Date, Discharge Type, Military Service Number, Purple Heart, POW, Combat, Agent Orange, and other similar related data. Collecting information such as medical and demographic information that will be used for eligibility and patients' medical treatment or health care services.

Yes **Medical Information**

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

Diagnostic information with regards to patient treatment history and future treatment. Also, clinical information from VA and DoD is used in the diagnosis and treatment of the veteran.

No **Criminal Record Information**

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

Yes **Guardian Information**

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

Used in the notification process and as required for medical decisions. Used to collect veteran cemetery information and NOK for emergency identification and notification.

NO y/n? **Education Information**

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

information.	
NA	
NO	<input type="checkbox"/> y/n? Rehabilitation Information
Specifically identify the personal information collected, and describe the intended use of the information.	
NA	
	<input type="checkbox"/> y/n? Other Personal Information (specify):
NA	
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.	

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: |

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

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

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

Yes **Veteran Source**

Information is obtained from the veteran for general, demographic, emergencies, financial, medical etc |

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

No **Public Source(s)**

Yes **VA Files and Databases**

Muse data base

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

IRS, SSA, DOD data used for income verification to determine if 3rd party collection is possible; used in determining eligibility for care; used in sharing of health care information with DOD.

No **State Agency Source(s)**

No **Local Agency Source(s)**

No **Other Source(s)**

		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

5.3 Collection Methods

Yes	Web Forms:	Information collected on Web Forms and sent electronically over the Internet to project systems.
-----	-------------------	--

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

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

VA Form 1010EZ – see the VA 10-10EZ Form from the Website: <https://www.1010ez.med.va.gov/sec/vha/1010ez/> |

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

No	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.
----	----------------------------------	---

Yes	Telephone Contact:	Information is collected via telephone.
-----	---------------------------	---

Veteran answer questions posed to them over the phone to collect the form 1010EZ data, to advise of appointments, to make changes to demographic information. These calls are usually initiated by an administrative clerk, clinical personnel, or by the veteran. The information used for updating purposes is entered in VistA.

No	Other Collection Method:	
----	---------------------------------	--

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 the data collection mandatory or voluntary?

Mandatory |

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

Notice of Privacy Practices and through the registration process upon enrollment. 1010EZ |

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

Ongoing |

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

Not applicable

No	Privacy notice is provided on each page of the application.
----	--

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

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

No **Web Forms:**

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

|

Yes **Paper Forms:**

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 veterans are informed that this information is collected for eligibility purposes and this conveyed to them via written notice. Also, patients fill out required fields of information on Form 1010 and an explanation of privacy policy is provided. Collection media will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements. In addition, the projects will identify opportunities for individuals to provide/decline consent and the consent methods will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements.

Yes **Electronic File Transfer:**

a) 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:

This project will connect to existing VA files and databases including VISTA, AAC and VA medical centers to continuously update veteran records and will serve as the ultimate, authoritative source of veteran id data.

No **Computer Transfer Device:**

a.) 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:

Yes **Telephone:**

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 veterans are informed that this information is collected for eligibility purposes and this privacy policy is conveyed to them via written notice annually. Also, information is obtained over the telephone interview and patients are provided with a consent form to sign and return. In addition, the projects will identify opportunities for individuals to provide/decline consent and the consent methods will adhere to VA existing practices, policies and procedures and Federal guidelines and requirements.

No **Other Method:**

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?

NO

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

No

5.6 Data Quality

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

This project will follow VA guidelines and will comply with federal regulatory requirements to develop appropriate data collection procedures and safeguard veteran id data. The form is electronic and validates the entry so that erroneous data is not taken.

Data is collected electronically based on the automation of VA forms and clinical procedures. Individuals may either visit the VAMC where they receive their care and begin the process or may visit the Freedom of Information Act (FOIA) Website for VA at <http://www.va.gov/oit/cio/foia/guide.asp#how> or may go through VA Forms at <http://www.va.gov/vaforms/medical/pdf/vha-10-5345-fill.pdf> . Further information regarding the VA SOR is available at http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf

5.6.b) How is data checked for completeness?

Data is reviewed by staff and compared to paper forms. For CM and RE, the specific steps and procedures to ensure data integrity and completeness have not yet been developed. However, parts of the projects are designed to verify the data for relevance, authenticity and accuracy prior to becoming part of the systems.

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

Throughout the medical center for veterans checking in for clinical appointments or for admissions, the demographic information is reviewed with the veteran. Administrative data is updated with each application for care. Pre-Registration staff contact veterans and update and/or verify information.

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

New data is compared with printed form or via patient verification. , the specific steps and procedures to ensure data relevancy, integrity and completeness have not yet been developed. However, parts of the projects are designed to verify the data for relevance, authenticity and accuracy prior to becoming part of the systems. .

PIA SECTIONS 6

Use and Disclosure

6.1 User Access and Data Sharing

6.1 User Access and Data Sharing

--> *Individuals - Access granted to individuals should be limited to the data needed to perform their assigned duties. List procedures to detect and deter browsing and unauthorized access.*

--> *Other Agencies – Any Federal, State or local agencies that have authorized access to collected personal information must be identified.*

--> *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. Check all applicable Individual/organizational access below.

Yes	System Users
Yes	System Owner, Project Manager
Yes	System Administrator
No	Contractor
Yes	Other Veteran Organization
Yes	Other Federal Agency
No	State Agency
No	Local Agency
Yes	Other System
No	Other User(s)

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

For RE and CM, users include VA staff who perform their normal duties necessary to support veteran contacts, system management and support, management, and maintenance functions will have access to the personal information. Procedures to detect and deter browsing and unauthorized access will be defined when the project moves to deployment or operational phase. The project plans to share the collected personal information with DoD and other authorized partners. Within VA, the new project potentially will share data with VA financial management system, VistA, VHA Health Data Repository (HDR). However, the exact systems to share data with and the control methods to ensure that only defined data are transmitted are not defined yet.

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

Access to the data will be role-based, specifically to limit access to the least amount necessary to perform the VA's normal duties and provide service to the veteran. compliance with the HIPAA Privacy Rule regulations. Access is limited to a need-to-know basis, either to

resolve complaints, or fix technical system problems.

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

The exact criteria, procedures, controls and responsibilities regarding access will be defined and documented at a later stage in the project.

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 based on job function.
A limited set of users--the VA Privacy Staff and top-level Privacy Officers--

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)

The RE and CM projects plan to develop training materials and privacy processes and guidelines to safeguard veteran ID data and prevent misuse. These training materials and processes will be documented and provided to all relevant users and will be monitored closely.

6.1.f) Do other systems share data or have access to data in this project's systems?

For CM and RE, yes.

6.1.f.1) If you have selected YES above, explain below. If you have selected NO above, then SKIP to section 6.2 'Data Quality'.

The project plans to share the collected personal information with DoD, DMDC, DEERS, VIS and other authorized partners. Within VA, the project potentially will share data with VA financial management system, VistA, VHA Health Data Repository (HDR).

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

Yes - VHA1605.1 and VHA 1605.2 VA HANDBOOKS

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

User access will be restricted only data relevant to specific needs will be accessed. Audits will be done to ensure users have appropriate keys.

6.1.i) 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.

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

Yes

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

Need to know is in place, and eventually role-based access is required. Likewise, all access to data within the system is logged and closely monitored. VA Privacy & Security training must be completed before access to information is allowed.

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

Data that is shared between DoD and VA and the protections that are apply are addressed in the DoD and VA sharing agreements. The need to know for clinical data with the DoD's system is the primary control that will ensure information is protected by both parties. Local Privacy Officer & ISO are responsible for ensuring information is protected.

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

Electronically and in paper format

6.1n) 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.

MOU is in place with external organizations who information is shared with. The agreement specifically identifies the information and how it will be protected.

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

Protected by the need to know; recipient agrees to follow VA privacy guidelines; VA privacy & security training required

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

Mandatory Privacy and Security training

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

6.2 Access to Records and Requests for Corrections

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

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

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

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

Individuals may either visit the VAMC where they receive their care and begin the process or may visit the Freedom of Information Act (FOIA) Website for VA at <http://www.va.gov/oit/cio/foia/g-uide.asp#how> or may go through VA Forms at <http://www.va.gov/vaforms/medical/pdf/vha-10-5345-fill.pdf>. Further information regarding the VA SOR is available at http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_-SOR_compilation.pdf. Individuals may request their own information through Release of Infomration.

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

| Same as above (6.2.b) |

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

| The patient is mailed a notice describing the process. |

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

7 Retention and Disposal

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

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

VA HBK 6300.1 Records Management Procedures explains the Records Control Schedule procedures.
System of Records Notices may be accessed via:
http://vawww.vhaco.va.gov//privacy/SystemofRecords.htm
or
http://vawww.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. Clinical information is retained in accordance with VA Records Control Schedule 10-1. Demographic information is updated as applications for care are submitted and retained in accordance with VA Records Control Schedule 10-1.

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

| Paper records are retired/archived at the end of the retention period and sent to the Federal Retirement Center; electronic records are kept indefinitely.

7.c) Where are procedures documented?

| VA Handbook 6300; Record Control Schedule 10-1 |

7.d) How are data retention procedures enforced?

| Enforced by the Records Managers and other Management Administrators; Electronic files are kept indefinitely

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

Yes

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

8 SECURITY

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

8.1 General Security Measures

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

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

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

Vista is monitored in compliance with VA 6500 handbook which identifies 451 controls that IT monitors on a regular basis. Some of which are annual and some weekly.

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

Yes

8.2 Project-Specific Security Measures

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

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

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

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

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

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

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

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

All federal agencies are required to follow NIST standards. VA Handbook 6500 implements the standards required in NIST 853. VA 6500 list the controls that are implemented.

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

None

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

NA

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."

10. CHILDREN'S ONLINE PRIVACY PROTECTION ACT

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

No

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

11. PIA CONSIDERATIONS

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

VistA-Legacy is a steady state project and is governed by existing policies and procedures. Likewise, VistA Foundations Modernization is contained within the same governing bodies and therefore, also governed by the same established policies and procedures. As a result of performing the PIA, emphasis and attention to the PIA requirements will be applied to preparing a data quality management plan, addressing security and privacy concerns including ensuring that collection of personal information contains appropriate consent and release information and developing comprehensive standard operating procedures (SOP). For the PVTS, as a result of the PIA, this system has improved the security of the licensing process, and strengthened the safeguard procedures in the training and user manual.

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

List of all users are maintained to ensure those employees do not have access to specific information by being issued inappropriate keys. Adpacs audit menus to ensure they are relative to the position held; keys not needed to perform specific duties are disabled.

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?

N	y/n?	The potential impact is high if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.
Y	y/n?	The potential impact is moderate if the loss of availability could be expected to have a serious adverse effect on operations, assets, or individuals.
N	y/n?	The potential impact is low 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?

N	y/n?	The potential impact is high if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.
Y	y/n?	The potential impact is moderate if the loss of integrity could be expected to have a serious adverse effect on operations, assets, or individuals.
N	y/n?	The potential impact is low 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?

N	y/n?	The potential impact is high if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.
Y	y/n?	The potential impact is moderate if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets, or individuals.
N	y/n?	The potential impact is low 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, Moderate, Moderate

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

Vista is backed up daily, tapes are stored in a secured location. If the system goes down historic data can be obtained to provide effective patient care. There is immediate backup to everything that is going on from the point of availability.

Ensuring information is not compromised & Confidentiality is a requirement of all employees who have access to patient information; known breaches are evaluated, sanctions enforced when applicable.

NIST 800-53 Security controls are implemented and if any known vulnerabilities are identified NIST Controls will be put in place to prevent incidents.

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

12. PUBLIC AVAILABILITY

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

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

1. Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an 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:

NA

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

13. ACCEPTANCE OF RESPONSIBILITY AND ACKNOWLEDGEMENT OF ACCOUNTABILITY:

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

Yes

13.2) **Project Manager/Owner Name and Date**

BK Hack 19 FEB 08
BK Hack, Director, IT Opns, Region 2

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

		SECTION INCOMPLETE
	X	SECTION COMPLETED
		I have completed and reviewed my responses in this section.
X	** NOTE:	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	2/1/08	Section Update Date