

**Privacy Impact Assessment /VISTA 2008  
Cheyenne VAMC**

<b>PRIVACY IMPACT ASSESSMENT 2008</b>	
<b>Part I. Project Identification and Determination of PIA Requirement</b>	
<b>1. PROJECT IDENTIFICATION: LOCAL AREA NETWORK (LAN)</b>	
<b>1.1) Project Basic Information:</b>	
1.1.a) Project or Application Name:	<b>VISTA Legacy System</b>
1.1.b) OMB Unique Project Identifier:	<b>029-00-01-11-01-1180-00</b>
1.1.c) Concise Project Description	
<p>The VistA Legacy system is comprised of three core platforms:</p> <ol style="list-style-type: none"> <li>1. InterSystems Cache on VMS [VMS/Cache].</li> <li>2. InterSystems Cache on VMS[VMS/Cache] on Linux ECX Shadow server</li> <li>3. InterSystems Cache on VMS[VMS/Cache] on Linux Servers.</li> </ol> <p>Test System consists of a single ES40 server, included are magnetic tape drives, disk drives, and back up power from whole room UPS system. The Shadow server (Read Only) consists of a single server that mirrors the production system residing in Denver and Sacramento RDC's. The RDC's [Denver and Sacramento are region 1] consists of server farms under the control of the Regional Data Vista Team. The national VistA Legacy software package runs on these three hardware platforms and operating systems, and is made up of over 100 software packages, all of which are used at the RDC [Regional Data Centers], and facilities. Each package is made up of multiple software programs. The systems reside in a locked, alarmed room at each physical location.</p> <p>Access to the system is via workstations operating on Windows-family Operating Systems (O/S) including Windows 2000 Professional, and Windows XP, thin client terminals, and various models of "dumb" terminals located throughout a Medical Center. Microsoft Windows client workstations connect to VistA Legacy over a Windows network using terminal emulation software and the Remote Procedure Call (RPC) Broker. There is access from the Intranet to both the VA's wide area network (WAN) and to the Internet via the VA Internet Gateways. VA-approved firewalls are positioned between the Intranet and the Internet Gateways. Digital Equipment Corporation (DEC) VT and other types of terminals connect to VistA Legacy via Ethernet and terminal servers.</p> <p>The VistA Legacy Kernel software provides identification and authentication, access control via menu management, and auditing of user actions. VA FileMan, VistA Legacy's database management software, in conjunction with the Kernel, provides data access control.</p> <p>Using the computer, the VA provider can access VistA-Legacy applications and meet a wide range of health care needs.</p> <p>Life Cycle Stage: <b>Operational/Maintenance</b></p>	
<b>1.2) Contact Information:</b>	
1.2.a) Person completing document:	LaRoy Books
Title:	Privacy Officer
Organization:	Cheyenne VAMC 442
Telephone:	(307) 778-7550 extension 7012
Email Address:	LaRoy.Books@va.gov
1.2.b) CIO	Michael Cartwright
Title:	Chief Information Officer
Organization:	OI&T/Cheyenne VAMC 442
Telephone Number:	(307) 772-7725
Email Address:	Michael.Cartwright@va.gov

**Privacy Impact Assessment /VISTA 2008  
Cheyenne VAMC**

1.2.C) System Administrator:	Sherri Vick
Title:	Vista System Administrator
Organization:	OI&T/Cheyenne VAMC 442
Telephone:	(307) 778-7357
Email Address:	Sherri.Vick@va.gov
1.2.d) ISO:	Jeff Ross
Title:	Information Security Officer
Organization:	OI&T/Cheyenne VAMC 442
Telephone Number:	(307) 778-7343
Email Address:	Jeff.Ross@va.gov
<b>Section 2. Determination of PIA Requirements:</b>	
<p><i>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.</i></p>	
2. a) Will the project collect and/or maintain personally identifiable information of the public in IT systems.	<b>YES</b>
2.b) Is this a PIV project collecting PII, including from Federal employees, contractors, and others performing work for VA? <b>PIV is not collected or maintained on this system.</b>	<b>NA</b>
2.c) Has a previous PIA been completed within the last three years? <b>No</b>	
2.d) Has any changes been made to the system since the last PIA? <b>No</b>	
<b>Section 2 Review:</b>	
Privacy Officer has reviewed and approved the responses in this section.	
Date of Review: November 5, 2008	
Privacy Officer: LaRoy Books (307) 778-7550 X7012	
<b>Part II Privacy Impact Assessment</b>	
<b>3. Project Description:</b>	
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. <b>All information is necessary in order to provide congressionally mandated health care for Veterans.</b>	
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	
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. <b>(48,653 employee &amp; 46,284 patients)</b>	
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. <b>(3) Operation/Maintenance</b>	
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. <b>Operational 10 plus years</b>	
<b>Section 3 Review:</b>	
Privacy Officer has reviewed and approved the responses in this section.	
Date of Review: November 5, 2008	
Privacy Officer: LaRoy Books (307) 778-7550 X7012	
<b>4. System of Records:</b>	

**Privacy Impact Assessment /VISTA 2008  
Cheyenne VAMC**

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? <b>YES</b>	
4.b1) Is the system data maintained under one or more approved System(s) of Records? <b>YES</b>	
(1) For each applicable System of Records, list: (1) The System of Records identifier (number). <b>79VA19, 24va19</b>	
(2) The name of the System of Records: <b>Veterans Health Information System and Technology Architecture (VISTA-VA), Patient Medical Records</b>	
(3) Provide the location where the specific applicable System of Records Notice(s) may be accessed (include the URL) <a href="http://vaww.vhaco.va.gov/privacy/Update_SOR/SOR24VA19.pdf">http://vaww.vhaco.va.gov/privacy/Update_SOR/SOR24VA19.pdf</a> <a href="http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf">http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf</a>	
4.b2) Have you read, and will the application comply with, all data management practices in the System of Records? <b>YES</b>	
4.b.3) Was the System(s) of Records created specifically for this project, or created for another project or system? <b>Created specifically for this System.</b>	
4.b.4) Does the System of Records Notice require modification? <b>Modification for this system of Records is NOT Required.</b>	
4.b.5) Describe the required modifications. <b>NONE</b>	
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. <b>NA</b>	
<b>Section 4 Review:</b>	
Privacy Officer has reviewed and approved the responses in this section.	
Date of Review: November 5, 2008	
Privacy Officer: LaRoy Books (307) 778-7550 X7012	
<b>5. Data Collection:</b>	
<b>5.1 Data Types and Data Uses</b>	
<i>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:</i>	
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.	
<i>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."</i>	
<b>YES</b>	Veteran's or Primary Subject's Personal Contact Information (name, address, telephone, etc) The most common data types that are captured and accessed on a regular basis by authorized individuals are first and last name, middle initial, DOB, SSN, and address. This patient information falls into two classes: administrative and clinical. Clinical information is used to diagnose, prescribe treatment and follow clinically the patient through his/her health care encounters. Administrative data is used to identify the veteran (SSN), correspond to/from (name and address), and determine eligibility (patient administrative info + SSA and IRS data).
<b>YES</b>	Other Personal Information of the Veteran or Primary Subject? Insurance Companies.
<b>NO</b>	Dependant Information
<b>YES</b>	Service Information? Military Service Information (Branch of service, discharge date, discharge type, service connection, medical conditions related to military service, etc). This information is collected to assess eligibility for VA healthcare benefits, type of healthcare needed.
<b>Yes</b>	Medical Information? VistA-Legacy applications and meet a wide range of health care data needs. The VistA-Legacy system collects a wide range of personal medical information for clinical diagnosis, treatment, patient evaluation, and patient care. Common types of personal medical information would include lab test results, prescriptions, allergies, medical diagnoses, vital signs, etc. The information is used to treat and care for the

**Privacy Impact Assessment /VISTA 2008  
Cheyenne VAMC**

	veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of the veteran.
<b>NO</b>	Criminal Record Information?
<b>YES</b>	Guardian Information? Next of kin, DNR instructions, health care proxy designation. This information is used in the notification process and as required for medical decisions.
<b>NO</b>	Education Information?
<b>YES</b>	Radiology Imaging – Radiology Orders and Exam Reports are stored within the Radiology Package. Pointers for the Image locations on the Jukebox and RAID also reside in VistA.
<b>YES</b>	Rehabilitation Information? Treatment notes, progress notes, clinical assessments, clinical diagnosis information is collected. Used in follow-up treatment and as part of the medical history.
<b>YES</b>	Other Personal Information? Next-of-kin information and emergency contact information, such as name and telephone number, is collected from the veteran to use to contact other individuals in case of an emergency. In addition insurance and employment information is available on the veteran for use in billing for care.
<b>Section 5.1 Review:</b>	
Privacy Officer has reviewed and approved the responses in this section.	
Date of Review: November 5, 2008	
Privacy Officer: LaRoy Books (307) 778-7550 X7012	
<b>5.2 Data Sources</b>	
<i>Identify the source(s) of the collected information.</i>	
<i>a) Select all applicable data source categories provided below.</i>	
<i>b) For each category selected:</i>	
<i>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.</i>	
<i>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.)</i>	
<i>Note: PIV projects should use the "Other Source(s)" data source.</i>	
<b>YES</b>	Veteran Source: Data used to identify the veteran, determine eligibility for care, schedule treatment and manage the provided
<b>NO</b>	Public Sources(s)
<b>YES</b>	Va Files and Databases: For VistA-Legacy, Patient Treatment File is used to store and make inquiries of personally identifiable information about the veteran, previous clinical records, clinical information, drug information as needed to provide treatment and reimbursement.
<b>YES</b>	Other Federal Agency Source(s) IRS,SSA, DoD data used for income verification to determine if third party collection is possible. Also used in determining eligibility for care.
<b>YES</b>	State Agency Source(s): Medicaid, Licensing Boards, Courts.
<b>YES</b>	Local Agency Sources (S) Local Hospital, Nursing Homes, Rehabilitation Centers, Hospice, Blood Banks, and Other health care related facilities.
<b>NO</b>	Other Sources(s)

**Privacy Impact Assessment /VISTA 2008  
Cheyenne VAMC**

Section 5.2 Review:		
Privacy Officer has reviewed and approved the responses in this section.		
Date of Review: November 5, 2008		
Privacy Officer: LaRoy Books (307) 778-7550 X7012		
<b>5.3 Collection Methods</b>		
<i>Identify and describe how personal information is collected:</i>		
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.		
<b>YES</b>	Web Forms	Information collected on Web Forms and sent electronically over the Internet to project systems.  The web form is located <a href="https://www.1010ez.med.va.gov/sec/vha/1010ez/showForm.asp">https://www.1010ez.med.va.gov/sec/vha/1010ez/showForm.asp</a> . This site from which this form is accessed ( <a href="http://www.va.gov">http://www.va.gov</a> ) references the VA Privacy and Security site ( <a href="http://www.va.gov/privacy">http://www.va.gov/privacy</a> ), as well as the VA Disclaimer site ( <a href="http://www.va.gov/disclaim.htm">http://www.va.gov/disclaim.htm</a> ) and the VA FOIA site ( <a href="http://vaww.va.gov/OIT/CIO/FOIA/default.asp">http://vaww.va.gov/OIT/CIO/FOIA/default.asp</a> ).
<b>YES</b>	Paper Forms	Information collected on Paper Forms and submitted personally, submitted via Postal Mail and/or submitted via Fax Machine. <b>VA Form 1010EZ</b>
<b>YES</b>	Electronic File Transfer	Information stored on one computer/system (not entered via a Web Form) and transferred electronically to project IT systems.  Radiology images are transferred between local hospitals and this VAMC, this is done by site2site VPN. Information is stored on the VISTA Imaging PACS System.
<b>YES</b>	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.  Digital medical images are acquired through standard image interfaces from medical devices or from cameras. Images are identified with the patient's medical record through use of the hospital information system database. In some cases, images or reports are provided on compact discs by the patients themselves; these are imported through the VistA Imaging interface.
<b>YES</b>	Telephone Contact	Information is collected via telephone.  Veterans answer questions posed over phone to collect Form 1010EZ data
<b>YES</b>	Other Collection Method	Information is collected through a method other than those listed above. Website URL: <a href="https://www.1010ez.med.va.gov/sec/vha/1010ez/showForm.asp">https://www.1010ez.med.va.gov/sec/vha/1010ez/showForm.asp</a> ; paper form: 1010EZ; computer transfer media: electronic file transfer and query. Telephone contact: patient telephones, enrollment staff, provides personal data to fill out 1010EZ, verbally approves use of data.
Section 5.3 Review:		
Privacy Officer has reviewed and approved the responses in this section.		
Date of Review: November 5, 2008		
Privacy Officer: LaRoy Books (307) 778-7550 X7012		
<b>5.4 Notice</b>		
<i>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.</i>		
5.4.a) Is personally identifiable information collected directly from individual members of the public and maintained in the project's IT systems? <b>YES</b>		
5.4.b) Is the data collection mandatory or voluntary? <b>Mandatory</b>		

**Privacy Impact Assessment /VISTA 2008  
Cheyenne VAMC**

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? <b>VA Form 1010EZ; VA Notice of Privacy Policies</b>		
5.4.d) Is the data collection new or ongoing? <b>Ongoing</b>		
5.4.e.1) If personally identifiable information is collected online, is a privacy notice provided that includes the following elements?		
<b>NO</b>	Not applicable	
<b>YES</b>	Privacy notice is provided on each page of the application.	
<b>YES</b>	A link to the VA Website Privacy Policy is provided.	
<b>YES</b>	Proximity and Timing: the notice is provided at the time and point of data collection.	
<b>YES</b>	Purpose: notice describes the principal purpose(s) for which the information will be used.	
<b>YES</b>	Authority: notice specifies the legal authority that allows the information to be collected.	
<b>YES</b>	Conditions: notice specifies if providing information is voluntary, and effects, if any, of not providing it.	
<b>YES</b>	Disclosures: notice specifies routine use(s) that may be made of the information.	
5.4.e.2) If necessary, provide an explanation on privacy notices for your system: 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")		
<b>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.</b>		
<i>Note: if PII is transferred from other projects, explain any agreements or understandings regarding notification of subjects</i>		
YES	Web Forms:	Patients are allowed to download Form 1010 which contains privacy information concerning each of the data fields they are required to enter.
YES	Paper Forms:	Patients fill out required fields of information on Form 1010 and an explanation of privacy policy provided.
NO	Electronic File Transfer:	
NO	Computer Transfer Device:	
YES	Telephone	Information is obtained over telephone interview and patients are provided with a consent form to sign and return.
YES	Other Method:	In person, verbal transfer of information.
Section 5.4 Review:		
Privacy Officer has reviewed and approved the responses in this section.		
Date of Review: November 5, 2008		
Privacy Officer: LaRoy Books (307) 778-7550 X7012		
<b>5.5 Consent for Secondary Use of PII:</b>		
<i>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.</i>		
5.5.a) Will personally identifiable information be used for any secondary purpose? <b>YES</b>		
<i>Note: If you have selected No above, then SKIP to question 5.6, "Data Quality."</i>		
Section 5.5 Review:		
Privacy Officer has reviewed and approved the responses in this section.		
Date of Review: November 5, 2008		
Privacy Officer: LaRoy Books (307) 778-7550 X7012		
<b>5.6 Data Quality</b>		
5.6.a) Explain how collected data are limited to required elements: Information requested is limited to that requested on the VA Form 1010EZ and that associated with health care and clinical procedures.		

**Privacy Impact Assessment /VISTA 2008  
Cheyenne VAMC**

5.6.b) How is data checked for completeness? Data is reviewed by staff and compared to paper forms	
5.6.c) What steps or procedures are taken to ensure the data are current and not out of date? Clinical data is not removed. Administrative data is updated with each application for care.	
5.6.d) How is new data verified for relevance, authenticity and accuracy? New data is compared with printed form or via patient verification	
Section 5.6 Review:	
Privacy Officer has reviewed and approved the responses in this section.	
Date of Review: November 5, 2008	
Privacy Officer: LaRoy Books (307) 778-7550 X7012	
<b>6. Use and Disclosure</b>	
<b>6.1 User Access and Data Sharing</b>	
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.	
<b>YES</b>	System Users
<b>YES</b>	System Owner: Region One RDC is owner of the equipment and has Admin rights
<b>YES</b>	System Administrator
<b>YES</b>	Contractor – Contractor accessing patient information are required to meet the same requirements as an employee; background investigation, Cyber Security and Privacy Training and signed Rules of Behavior.
<b>YES</b>	Other Veteran Organization – Veterans Benefits Administration (VBA)
<b>YES</b>	Other Federal Agency- There is certain VHA VistA patient data that is shared with DOD through the Federal/Bidirectional Health Information Exchange (FHIE/BHIE) Program under DUAs that have been in effect for over three years. In addition, certain clinical information is being shared with CDC, also under an established DUA.
<b>NO</b>	State Government Agency
<b>NO</b>	Local Government Agency
<b>NO</b>	Other Projects/Systems
<b>YES</b>	Other User(s)- There is certain VHA VistA patient data that is shared with DOD through the Federal/Bidirectional Health Information Exchange (FHIE/BHIE) Program under DUAs that have been in effect for over three years. In addition, certain clinical information is being shared with CDC, also under an established DUA. Additionally, State Veterans Homes will have access to this information.
If information is shared with persons or organization(s) that are not described by the categories provided, use this field to identify and describe what other persons or organization(s) have access to personal information stored on project systems. Also, briefly describe the data sharing	
6.1.a.1) Describe here who has access to personal information maintained in project's IT systems: Clinical and administrative staff involved in the provision of care.	
6.1.b) How is access to the data determined? <b>On a need to know basis</b>	

**Privacy Impact Assessment /VISTA 2008  
Cheyenne VAMC**

6.1.c) Are criteria, procedures, controls, and responsibilities regarding access documented? If so, identify the documents. YES-VHA1605.1 and VHA 1605.2 VA Handbooks	
6.1.d) Will users have access to all data on the project systems or will user access be restricted? Explain. <b>Restricted</b> - Users will only have access needed to perform their job.	
6.1.e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by those having access? (Please list processes and training materials that specifically relate to unauthorized browsing) Processes and training materials specifically related to preventing misuse, including violation of unauthorized browsing are currently being developed and projected to be available next FY.	
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) <b>YES. State Veterans Homes and veteran's organizations such as VBA when consent for access is granted by the veteran.</b>	
<b>Note: If you have selected No above, then SKIP to question 6.2, "Access to Records and Requests for Corrections".</b>	
Section 6.1 Review:	
Privacy Officer has reviewed and approved the responses in this section.	
Date of Review: November 5, 2008	
Privacy Officer: LaRoy Books (307) 778-7550 X7012	
<b>6.2 Access to Records and Requests for Corrections</b>	
<i>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.</i>	
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.) <a href="http://www1.va.gov/vhapublications/viewpublication.asp?pub_id=1089">http://www1.va.gov/vhapublications/viewpublication.asp?pub_id=1089</a>	
<b>YES</b>	The internet site will provide a link that leads to their information. See 6.2.b)
<b>YES</b>	The internet site will provide, via link, written instructions on how to amend their information. <a href="http://www1.va.gov/vhapublications/viewpublication.asp?pub_id=1089">http://www1.va.gov/vhapublications/viewpublication.asp?pub_id=1089</a>
<b>YES</b>	The internet site will provide a phone number of a VA representative who will provide instructions.
<b>YES</b>	The application will use other method (explain below).
<b>NO</b>	The application is exempt from needing to provide access.
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 <a href="http://www.va.gov/oit/cio/foia/guide.asp">http://www.va.gov/oit/cio/foia/guide.asp</a> how or may go through VA Forms at <a href="http://www.va.gov/vaforms/medical/pdf/vha-10-5345-fill.pdf">http://www.va.gov/vaforms/medical/pdf/vha-10-5345-fill.pdf</a> . Further information regarding the VA SOR is available at <a href="http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf">http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf</a> .	
6.2.c) What are the procedures for correcting erroneous information? <b>Same as above</b>	
6.2.d) If no redress is provided, are alternatives available? <b>NA</b>	
6.2.e) Provide here any additional explanation; if exempt, explain why the application is exempt from providing access and amendment. <b>The patient is mailed a notice describing the process.</b>	
Section 6.2 Review:	
Privacy Officer has reviewed and approved the responses in this section.	
Date of Review: November 5, 2008	
Privacy Officer: LaRoy Books (307) 778-7550 X7012	
<b>7. Retention and Disposal</b>	
<i>By completing this section, you provide documented assurance that proper data retention and disposal practices are in place.</i>	

**Privacy Impact Assessment /VISTA 2008  
Cheyenne VAMC**

<p><i>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.</i></p>	
<p>VA HBK 6300.1 Records Management Procedures explains the Records Control Schedule procedures. <a href="http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&amp;FTtype=2">http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&amp;FTtype=2</a></p>	
<p>System of Records Notices may be accessed via: <a href="http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm">http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm</a> Or <a href="http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf">http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf</a></p>	
<p>For VHA projects, VHA Handbook 1907.1 (Section 6j) and VHA Records Control Schedule 10-1 provide more general guidance. <a href="http://vaww1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1469">http://vaww1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1469</a> and VHA Records Control <a href="http://www1.va.gov/vhapublications/RCS10/rcs10-1.pdf">http://www1.va.gov/vhapublications/RCS10/rcs10-1.pdf</a></p>	
<p><i>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.</i></p> <p>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.</p>	
<p><i>7.b) What are the procedures for eliminating data at the end of the retention period?</i></p> <p>Electronic Final Version of Patient Medical Record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records Control Schedule 10-1, Item XLIII, 2.b. (Page 190). At the present time, VistA Imaging retains all images. We are performing a study to explore whether some images can be eliminated on an earlier schedule.</p>	
<p><i>7.c) Where are procedures documented? VA Handbook 6300.01 at:</i> <a href="http://vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&amp;FTtype=2">http://vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&amp;FTtype=2</a> and VHA Records Control <a href="http://www1.va.gov/vhapublications/RCS10/rcs10-1.pdf">http://www1.va.gov/vhapublications/RCS10/rcs10-1.pdf</a></p>	
<p><i>7.d) How are data retention procedures enforced? VA Records Control Schedule 10-1 (page 8):</i></p> <p>Records Management Responsibilities</p> <p>The Health Information Resources Service (HIRS) is responsible for developing policies and procedures for effective and efficient records management throughout VHA. In addition, HIRS acts as the liaison between VHA and National Archives and Records Administration (NARA) on issues pertaining to records management practices and procedures.</p> <p>Chief of Health Information Management is responsible for records management activities at their facilities.</p> <p>Program officials are responsible for creating, maintaining protecting, and disposing of records in their program area in accordance with NARA regulations and VA policy.</p> <p>All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures. Disposition of Records.</p>	
<p><b>Section 7 Review:</b></p>	
<p>Privacy Officer has reviewed and approved the responses in this section.</p>	
<p>Date of Review: November 5, 2008</p>	
<p>Privacy Officer: LaRoy Books (307) 778-7550 X7012</p>	
<p><b>8. General Security Measures</b></p>	
<p><i>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</i></p>	
<p><i>8.1.a) Per OMB guidance, citing requirements of the Federal Information Security Management Act, address the following items (select all applicable boxes.):</i></p>	
<b>YES</b>	The project is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured.
<b>YES</b>	The project has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.
<b>YES</b>	Security monitoring, testing, and evaluating are conducted on a regular basis to ensure that controls continue to work properly, safeguarding the information.

**Privacy Impact Assessment /VISTA 2008  
Cheyenne VAMC**

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

OI&T manages and monitors Department-wide security solutions, such as anti-virus protection, authentication, independent vulnerability scanning and penetration testing, and intrusion detection systems. Each year an annual security self-assessment survey is conducted as part of the VA's IT security framework, with this project completing its FISMA Assessment in August 2007. The results of the assessment are used by the VA CIO to develop Department-wide remediation priorities. Additionally, the VistA program manager uses the survey results to evaluate the adequacy of safeguards on the system, and ensure that the system is adequately funded for security needs. The VistA Security Plan is updated periodically to reflect the results of IT security controls adopted for implementation through the annual FISMA Assessment. At the close of the assessment period, appendices of security controls selected for the system, as well as controls that are either temporarily or permanently suspended as a result of the System Owner's risk-based decisions, are generated. VistA has gone through the C&A process, including testing of operational, technical and management security controls. IT security for the VistA System is also provided through education ensuring users are aware of the risks associated with computer security. In addition, the OI&T performs onsite review and inspection division OI&T Compliance audits at VA facilities including testing of the effectiveness of management, technical and operational IT security controls related to facility systems. Any noted deficiencies are entered into the FISMA POA&M database. VA's Network and Security Operations Center (NSOC) monitors VA networks through IDS sensors, ensuring that suspicious events are detected, analyzed, and handled appropriately. The NSOC works collaboratively with Information Security Officers (ISOs) at all VA locations to report and/or follow up on suspicious network activity captured by IDS sensors. The VA-CIRC is the central coordinating and response office for all cyber security incidents affecting the VA. The VA-CIRC identifies, validates, and directs all response efforts, and coordinates efforts with government incident response centers including US-CERT.

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

**8.2 Project-Specific Security Measures**

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

*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? Is so, describe these controls.*

This VA VAMC is following IT security requirements as described in the FISMA, and outlined in NIST 800-53. 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 August 2007. The Office of Information Technology (OI&T) provides regular guidance on IT security issues and interpretation of rules and regulations set by legislation, policy or NIST guidelines. OI&T will serve as a point of contact for additional questions or specifics on implementation of security measures. The VISTA System at this facility does not have its own security controls, independent of the VA network.

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

At the Department level the CIO's Office of Office of Information and Technology (OI&T) is responsible for the establishment of directives, policies, & procedures which are consistent with the provisions of Federal Information Security Management Act (FISMA) as well as guidance issued by the Office of Management & Budget (OMB), the National Institute of Standards & Technology (NIST), & other requirements that VistA-Legacy is and has been subject to. In addition, OCIS administers and manages Department-wide security solutions, such as anti-virus protection, authentication, vulnerability scanning & penetration testing, & intrusion detection systems, and incident response (800-61). At the VistA-Legacy project level -The Project Manager ensures that CIO-provided security directives are integrated into the project's security plan & implemented by VA & contractor staff throughout the project Funding needs are dependent on IT security requirements identified in the system development life cycle (800-64) (i.e. risk assessments (800-30), certification and accreditation (800-37 and 800-53), as well as identified security weaknesses that must be corrected.

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

**Privacy Impact Assessment /VISTA 2008  
Cheyenne VAMC**

Management, Operational, and Technical Controls that are currently in place but may not yet be entirely NIST 800-53 compliant.
8.2.d) Explain what security controls are being used to mitigate these risks.
Controls that are consistent with NIST 800-53.
<b>Section 8 Review:</b>
Privacy Officer has reviewed and approved the responses in this section.
Date of Review: November 5, 2008
Privacy Officer: LaRoy Books (307) 778-7550 X7012
<b>9. Change Record</b>
<i>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</i>
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). N/A
<b>If no, then proceed to Section 10, "Children's Online Privacy Protection Act."</b>
<b>Section 9 Review:</b>
Privacy Officer has reviewed and approved the responses in this section.
Date of Review: November 5, 2008
Privacy Officer: LaRoy Books (307) 778-7550 X7012
<b>10. Children's Online Privacy Protection Act</b>
10.a) Will information be collected through the Internet from children under age 13? <b>NO</b>
<b>If "No" then Skip to Section 11, "PIA Considerations".</b>
<b>Section 10 Review:</b>
Privacy Officer has reviewed and approved the responses in this section.
Date of Review: November 5, 2008
Privacy Officer: LaRoy Books (307) 778-7550 X7012
<b>11. PIA Assessment</b>
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.
Vista-Legacy is a steady state project and is governed by existing policies and procedures and they are already in place. No change or choices resulted from doing this PIA
11b) What auditing measures and technical safeguards are in place to prevent misuse of data?
Auditing measures and technical safeguards that are consistent with NIST 800-53 and FISMA requirements.
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?
<b>YES</b> The potential impact is <u>high</u> if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.
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?
<b>YES</b> The potential impact is <u>high</u> if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.
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?

**Privacy Impact Assessment /VISTA 2008  
Cheyenne VAMC**

<b>YES</b>	<b>The potential impact is <u>high</u> if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.</b>
11f) What was the highest impact from questions 11c, 11d, and 11e? <b>HIGH</b>	
11g) What controls are being considered for this impact level? <b>Management, Technical, and Operational Controls as outlined in NIST 800-53</b>	
Section 11 Review:	
Privacy Officer has reviewed and approved the responses in this section.	
Date of Review: November 5, 2008	
Privacy Officer: LaRoy Books (307) 778-7550 X7012	
<b>12. PUBLIC AVAILABILITY</b>	
<i>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.</i>	
<i>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).</i>	
<i>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).</i>	
<i>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.</i>	
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? <b>NO</b>	
Section 12 Review:	
Privacy Officer has reviewed and approved the responses in this section.	
Date of Review: November 5, 2008	
Privacy Officer: LaRoy Books (307) 778-7550 X7012	

**Privacy Impact Assessment /VISTA 2008  
Cheyenne VAMC**

**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.*

\_\_\_\_\_ **Date** November 5, 2008  
2008  
LaRoy Books  
Privacy Officer

\_\_\_\_\_ **Date** November 5,  
2008  
Jeff Ross  
Information Security Officer

\_\_\_\_\_ **Date** November 5, 2008  
2008  
Sherri Vick  
System Administrator

\_\_\_\_\_ **Date** November 5,  
2008  
Michael Cartwright  
CIO ITS

Approve

\_\_\_\_\_ **Date** November 5, 2008  
David M. Kilpatrick M.D.  
Medical Center Director  
Cheyenne, WY