

**Privacy Impact Assessment 2008 / VISTA  
VA Montana Healthcare System**

<b>Part I. Project Identification and Determination of PIA Requirement</b>	
<b>1. PROJECT IDENTIFICATION: Veterans Health Information Systems and Technology Architecture (VISTA)</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 used for the storage of clinical (patient and employee), financial and administration information. It 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 and Miles City VA clinic Legacy system consists of a single Alpha 4100 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. 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>Bar Code Medication Administration (BCMA) back up- a smaller version of VISTA that communicates with the main VISTA system through HL 7 protocols.</p> <p>Using the computer, the VA provider can access VISTA-Legacy applications and meet a wide range of health care needs. Life Cycle Stage: <b>Operational/Maintenance.</b></p>	
<b>1.2) Contact Information:</b>	
<b>1.2.a) Person completing this document:</b>	<b>Lesa Wallis</b>
<b>Title:</b>	Privacy / FOIA Officer
<b>Organization:</b>	VA Montana Healthcare System 436
<b>Telephone Number:</b>	(406) 447-7670
<b>Email Address:</b>	Lesa.Wallis@va.gov
<b>1.2.b) CIO /Project Manager:</b>	<b>Paul Gauthier</b>
<b>Title:</b>	Chief Information Officer
<b>Organization:</b>	OI&T / VA Montana Healthcare System
<b>Telephone Number:</b>	(406) 447-7673
<b>Email Address:</b>	Paul.Gauthier@va.gov

**Privacy Impact Assessment 2008 / VISTA  
VA Montana Healthcare System**

<b>1.2.c) System Administrator:</b>	<b>Doug Enghusen</b>
<b>Title:</b>	VISTA System Administrator
<b>Organization:</b>	OI&T / VA Montana Healthcare System
<b>Telephone Number:</b>	(406) 447-7907
<b>Email Address:</b>	Doug.Enghusen@va.gov
<b>1.2.d) ISO:</b>	<b>William Rau</b>
<b>Title:</b>	Information Security Officer
<b>Organization:</b>	OI&T / VA Montana Healthcare System
<b>Telephone number:</b>	(406) 447-7100
<b>Email Address:</b>	William.Rau@va.gov

**2. DETERMINATION OF PIA REQUIREMENTS:**

A privacy impact assessment (PIA) is required for all VA projects with IT systems that collect, maintain, and/or disseminate personally identifiable information (PII) of the public, not including information of Federal employees and others performing work for VA (such as contractors, interns, volunteers, etc.), unless it is a PIV project. All PIV projects collecting any PII must complete a PIA. PII is any representation of information that permits the identity of an individual to be reasonably inferred by either direct or indirect means. Direct references include: name, address, social security number, telephone number, email address, financial information, or other identifying number or code. Indirect references are any information by which an agency intends to identify specific individuals in conjunction with other data elements. Examples of indirect references include a combination of gender, race, birth date, geographic indicator and other descriptors.

2.a) Will the project collect and/or maintain personally identifiable information 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>NO</b>
<b><i>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.</i></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 last PIA?	<b>NO</b>

**Section 2 Review:**

Privacy Officer has reviewed and approved the responses in this section		
Date of Review: March 19, 2008	2 <sup>nd</sup> draft completed: May 8, 2008	3 <sup>rd</sup> draft completed May 28, 2008
Privacy Officer: Lesa Wallis (406) 447-7670		

**Part II. Privacy Impact Assessment**

**3. PROJECT DESCRIPTION:**

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

3.a) Provide a concise description of why personal information is maintained for this project, such as determining eligibility for benefits or providing patient care. <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? <b>38 US Code, Section 7301</b>

**Privacy Impact Assessment 2008 / VISTA  
VA Montana Healthcare System**

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. **98,765 Patients and 56,489 New users (employees, remote access users, past and current employees)**

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

3.e) Identify either the approximate date (MM/YYYY) the project/system will be operational (if in the design or development stage), or the approximate number of years that the project/system has been in operation.  
**Operational 10 plus years**

**Section 3 Review:**

Privacy Officer has reviewed and approved the responses in this section.

Date of Review: March 19, 2008      2<sup>nd</sup> draft completed: May 8, 2008      3<sup>rd</sup> draft completed May 28, 2008

Privacy Officer: Lesa Wallis (406) 447-7670

**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), **79VA19, 23VA163, 24VA19, 24VA136, 77VA10Q, 88VA244, 89VA19, 97VA105, 100VA10NS10, 113VA112, 114VA16**

(2) The name of the System of Records, and **Veterans Health Information Systems and Technology Architecture (VISTA) Records, Non-VA Fee Basis Records, Patient Medical Records, Patient Medical Records, Healthcare Provider Credentialing and Privileging Records, Accounts Receivable Records, Health Eligibility Records, Consolidated Data Information System, Patient Representation Program Records, Telephone Care and Service Records, The Revenue Program- Billing and Collections Records**

(3) Provide the location where the specific applicable System of Records Notice(s) may be accessed (include the URL). <http://vaww.vhaco.va.gov/privacy/SystemofRecords>

4.b.2) Have you read, and will the application comply with, all data management practices in the System of Records Notice(s)? **YES**

4.b.3) Was the System(s) of Records created specifically for this project, or created for another project or system?  
**Created specifically for this system.**

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

**Privacy Impact Assessment 2008 / VISTA  
VA Montana Healthcare System**

4.b.4) Does the System of Records Notice require modification? **NOT required**

**Section 4 Review:**

Privacy Officer has reviewed and approved the responses in this section.

Date of Review: March 19, 2008

2<sup>nd</sup> draft completed: May 8, 2008

3<sup>rd</sup> draft completed May 28, 2008

Privacy Officer: Lesa Wallis (406) 447-7670

**5. DATA COLLECTION:**

**5.1 Data Types and Data Uses**

FIPS 199 establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization. Identify the types of personal information collected and the intended use(s) of that data:

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

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

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

YES	Veteran's or Primary Subject's Personal Contact Information (name, address, telephone, etc) <b>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) and for payment of healthcare.</b>
NO	Other Personal Information of the Veteran or Primary Subject?
NO	Dependent Information?
YES	Service Information? <b>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	Medical Information? <b>VISTA-Legacy applications and to 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 veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of the veteran.</b>
NO	Criminal Record Information?
YES	Guardian Information? <b>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	Education Information?
YES	Rehabilitation Information? <b>Treatment notes, progress notes, clinical assessments, clinical</b>

**Privacy Impact Assessment 2008 / VISTA  
VA Montana Healthcare System**

	<b>diagnosis information is collected. Used in follow-up treatment and as part of the medical history..</b>
<b>YES</b>	<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>
<b>YES</b>	<b>Other Personal Information (specify): 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:**  
 Privacy Officer has reviewed and approved the responses in this section.  
 Date of Review: March 19, 2008      2<sup>nd</sup> draft completed: May 8, 2008      3<sup>rd</sup> draft completed May 28, 2008  
 Privacy Officer: Lesa Wallis (406) 447-7670

**5.2 Data Sources**  
**Identify the source(s) of the collected information.**  
**a) Select all applicable data source categories provided below.**  
**b) For each category selected:**  
**i) Specifically identify the source(s) - identify each specific organization, agency, or other entity that is a source of personal information. ii) Provide a concise description of why information is collected from that source(s). iii) Provide any required additional clarifying information.**  
**Your responses should clearly identify each source of personal information, and explain why information is obtained from each identified source. (Important Note: This section addresses sources of personal information; Section 6.1, "User Access and Data Sharing" addresses sharing of collected personal information.)**

<b>YES</b>	<b>Veteran Source? Data used to identify the veteran, determine eligibility for care, schedule treatment, manage healthcare and payment or reimbursement of authorized healthcare.</b>
<b>NO</b>	<b>Public Source(s)?</b>
<b>YES</b>	<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>
<b>YES</b>	<b>Other Federal Agency Source(s)? IRS, SSA, DoD data used for income verification to determine if third party collection is possible and used in determining eligibility for care.</b>
<b>YES</b>	<b>State Agency Source(s)? Medicaid, Licensing Boards, Courts used for determining eligibility of benefits and identification of authorized patient representatives.</b>
<b>YES</b>	<b>Local Agency Source(s)? Local Hospital, Nursing Homes, Rehabilitation Centers, Hospice, Blood Banks, and Other health care related facilities for the continuation of patient care and treatments.</b>
<b>NO</b>	<b>Other Source(s)?</b>

**Section 5.2 Review:**  
 Privacy Officer has reviewed and approved the responses in this section.  
 Date of Review: March 19, 2008      2<sup>nd</sup> draft completed: May 8, 2008      3<sup>rd</sup> draft completed May 28, 2008  
 Privacy Officer: Lesa Wallis (406) 447-7670

**5.3 Collection Methods**  
**Identify and describe how personal information is collected:**  
**a) Select all applicable collection methods below. If the provided collection methods do not adequately describe a**

**Privacy Impact Assessment 2008 / VISTA  
VA Montana Healthcare System**

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.

YES	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://vawww.va.gov/OIT/CIO/FOIA/default.asp">http://vawww.va.gov/OIT/CIO/FOIA/default.asp</a> ).
YES	Paper Forms	Information collected on Paper Forms and submitted personally, submitted via Postal Mail and/or submitted via Fax Machine or treatment billing invoices. <b>Business Office for enrollment and benefits, via, VA Form 1010EZ and Means Test, via, VA Form 10-10-EZR. Information for payment or reimbursement of healthcare collected, via, health insurance claims HCFA 1500 and UB92 submitted from and mailed to outside providers.</b>
NO	Electronic File Transfer	
NO	Computer Transfer Device	
YES	Telephone Contact	Information is collected via telephone. <b>Enrollment and Eligibility of benefits – VA staff call veterans to obtain clarification or additional information on the VA Form 10-10EZ and 10-10EZR. Payment and Reimbursement of healthcare - VA staff call healthcare providers to obtain clarification on billing information and, request additional medical records for payment reviews. Veterans telephone VA to report medical treatment sought at non-VA facilities and to initiate VA payment of this treatment. For all examples, VA staff may collect the veteran's name, last 4 of SSN, verification of home address, date of treatments, financial data, employment data, military service data and VA service-connection awards.</b>
NO	Other Collection Method	

**Section 5.3 Review:**

Privacy Officer has reviewed and approved the responses in this section.

Date of Review: March 19, 2008      2<sup>nd</sup> draft completed: May 8, 2008      3<sup>rd</sup> draft completed May 28, 2008

Privacy Officer: Lesa Wallis (406) 447-7670

**5.4 Notice**

The Privacy Act of 1974 and VA policy requires that certain disclosures be made to data subjects when information in identifiable form is collected from them. The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

5.4.a) Is personally identifiable information collected directly from individual members of the public and maintained in the project's IT systems? **YES**

5.4.b) Is the data collection mandatory or voluntary? **Mandatory**

5.4.c) How are the individuals involved in the information collection notified of the Privacy Policy and whether provision of the information is mandatory or voluntary? **This is stated on the VA Form 1010EZ- VA Notice of Privacy Policies.**

**Privacy Impact Assessment 2008 / VISTA  
VA Montana Healthcare System**

5.4.d) Is the data collection new or ongoing? <b>Ongoing</b>	
5.4e.1) If personally identifiable information is collected online, is a privacy notice provided that includes the following elements?	
	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: <b>N/A</b>	
5.4.f) For each type of collection method used (identified in Section 5.3, "Collection Method"), explain:	
a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided. .	
<b>YES</b>	<b>Web Forms?: <u>Enrollment and Eligibility of benefits</u> – The VA Form 10-10EZ and 10-10EZR each have a section on the forms that states the purpose for data collection and usage and a Privacy Act statement. Veterans are also informed, via form instructions, whether disclosure is mandatory.</b>
<b>YES</b>	<b>Paper Forms?: <u>Enrollment and Eligibility of benefits</u> – VA staff collects data directly from veterans on the VA Form 10-10EZ and 10-10EZR. Each form has a section that states the purpose for data collection and usage and a Privacy Act statement. Veterans are also informed, via form instructions, whether disclosure is mandatory. <u>Payment and Reimbursement of healthcare</u> –Information is collected, via use of HCFA 1500 and UB92 medical claim forms used by VA and submitted by non-VA healthcare providers. Both forms contain a notice about collection and use of the information and they both contain Privacy Act statements for the users and recipients to read.</b>
<b>NO</b>	Electronic File Transfer?:
<b>NO</b>	Computer Transfer Device?:
<b>YES</b>	<b>Telephone?: <u>Enrollment and Eligibility of benefits</u> – The VA Form 10-10EZ and 10-10EZR are initially provided to veterans by mail. Then, upon receipt, VA staff may telephone veterans to provide additional information or clarifications. When veterans, manually fill out the form or fill it out on a web site, they may read the notice provided on the forms, explaining the purpose for the collection and usage of that information. <u>Payment and Reimbursement of healthcare</u> - Upon receipt of HCFA 1500 or UB92 medical claim forms, VA staff may telephone veterans and non-VA healthcare providers to collect additional billing information, verify data or obtain clarifications. Veterans may verbally inquire on the purpose and usage of this information. They would be provided a verbal answer. If a Privacy notice is requested, this would be mailed to the veteran. Non-VA healthcare providers would already have been informed of the purpose and usage of the data collection and a Privacy Act statement located on the forms themselves.</b>
<b>NO</b>	Other Method?:
<b>Section 5.4 Review:</b>	
Privacy Officer has reviewed and approved the responses in this section.	

**Privacy Impact Assessment 2008 / VISTA  
VA Montana Healthcare System**

Date of Review: March 19, 2008	2 <sup>nd</sup> draft completed: May 8, 2008	3 <sup>rd</sup> draft completed May 28, 2008
Privacy Officer: Lesa Wallis (406)447-7670		

**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 Research is not conducted at this facility. We do report statistical data to State Cancer Tumor Registry, otherwise if individual veteran's are participating in research studies at other VA's or private centers, then requests for VA data would be made in writing, with veteran permission, by the originating research organization.**

**Section 5.5 Review:**

Privacy Officer has reviewed and approved the responses in this section.

Date of Review: March 19, 2008	2 <sup>nd</sup> draft completed: May 8, 2008	3 <sup>rd</sup> draft completed May 28, 2008
Privacy Officer: Lesa Wallis (406) 447-7670		

**5.6 Data Quality**

5.6.a) Explain how collected data are limited to required elements: **As a business practice, information requested is limited to the data needed to complete the VA Form 10-10EZ and 10-10EZR and to carry out health care and clinical procedures, billing and payment of healthcare..**

5.6.b) How is data checked for completeness? **Information is reviewed and verified before saved by the user.**

5.6.c) What steps or procedures are taken to ensure the data are current and not out of date? **Clinical data - is reviewed for accuracy by users. Veterans may also request an amendment to their health records to have information deleted or corrected. Payment data - is reviewed for accuracy by the applicable users and periodic patches are installed to VISTA for current industry standard healthcare coding and pricing values.**

5.6.d) How is new data verified for relevance, authenticity and accuracy? **The users review new data received or entered within their applications to determine relevance, and accuracy. Also for Enrollment and Eligibility of benefits - New data is compared against data entered to printed forms such as the VA Form 10-10EZ and 10-10EZR or by individual verification. This is done by VA staff either by telephone or in-person meeting.**

**Section 5.6 Review:**

Privacy Officer has reviewed and approved the responses in this section.

Date of Review: March 19, 2008	2 <sup>nd</sup> draft completed: May 8, 2008	3 <sup>rd</sup> draft completed May 28, 2008
Privacy Officer: Lesa Wallis (406)447-7670		

**6. Use and Disclosure**

**6.1 User Access and Data Sharing**

**Identify the individuals and organizations that have access to system data.**

--> **Individuals - Access granted to individuals should be limited to the data needed to perform their assigned duties. Individuals with access to personal information stored in project system must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to prevent as well as detect unauthorized access and browsing.**

--> **Other Agencies – Any Federal, State or local agencies that have authorized access to collected personal information must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to protect personal information.**

--> **Other Systems – Information systems of other programs or projects that interface with the information system(s) of this project must be identified and the transferred data must be defined. Also, the controls that are in place to ensure that only the defined data are transmitted must be defined.**

6.1.a) Identify all individuals and organizations that will have access to collected information. Select all applicable

**Privacy Impact Assessment 2008 / VISTA  
VA Montana Healthcare System**

items below.	
YES	System Users? <b>Only system users are authorized access to specific folders</b>
YES	System Owner, Project manager? <b>Region One RDC is owner of the equipment and has Admin rights</b>
YES	Systems Administrator?
YES	Contractor? <b>Contractors accessing patient information must meet the same training and security requirements as an employee; background investigation, Cyber Security and Privacy Training and signed Rules of Behavior. The following contracts use or are exposed to PHI: Contract # <u>V259P-0258- PT for Miles City NH &amp; V259P-0259 PT for Miles City NH</u>- fee physical therapist for patients has access to VISTA for treatment documentation. <u>V436P-3655B Primary care to Billings clinic / St Vincent Healthcare</u>- providing staff to VA clinic; access to VISTA CPRS for treatment documentation. <u>V436P-3685</u> contracted provider of radiology services upon VA referral. Would be provided copy of VISTA CPRS consult (medical data) for authorization and instruction on type of service needed. <u>V259-P-0135</u> contracted clinic site with VA clerk and contracted MD. <u>V259-P-0113</u> Mental Health case management upon VA referral. Would be provided copy of VISTA CPRS consult (medical data) for authorization and instruction on type of service needed. <u>VA259-P-0188</u> contracted clinic site with VA clerk and contracted MD; access to VISTA CPRS for treatment documentation.</b>
NO	Internal Sharing: Veteran Organization?
NO	Other Veteran Organization?
YES	Other Federal Government Agency? <b>There is certain 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. Common patient clinical medical record data (treatments and diagnosis data). VA has access to DOD treatment records, they do not have access to VA records. CDC, also under an established DUA. Statistical infection control data (positive PPD tests, percentage of PPD tested staff etc)</b>
NO	State Government Agency?
NO	Local Government Agency?
NO	Other Project/ System?
NO	Other User(s)?
6.1.a.1) Describe here who has access to personal information maintained in project's IT systems: <b>Clinical and administrative staff involved in the provisions of healthcare, billing and payment of healthcare.</b>	
6.1.b) How is access to the data determined? <b>On a need to know basis.</b>	
6.1.c) Are criteria, procedures, controls, and responsibilities regarding access documented? If so, identify the documents. <b>Center Circular 04C-05-01</b>	
6.1.d) Will users have access to all data on the project systems or will user access be restricted? Explain. <b>Restricted access to project system. Users will only have access needed to perform their job, however, individual records contained within the system are not restricted.</b>	
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) <b>Center Circular 04C-05-01 and VA MT Healthcare System Rules of Behavior</b>	
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</b>	
6.1.g) Identify the measures taken to protect the privacy rights of the individuals whose data will be shared. <b>All</b>	

**Privacy Impact Assessment 2008 / VISTA  
VA Montana Healthcare System**

users, including contractors, are required to take Cyber Security training and Web-based Privacy Policy training prior to gaining access. The National Rules of Behavior are incorporated into Cyber Security training. Access is approved, granted and restricted to only authorized users.

6.1.h) Identify who is responsible, once personal information leaves your project's IT system(s), for ensuring that the information is protected. **The recipient of the personal information, contractors, VA staff, other govt agency staff, is held responsible for protections while in their possession, following Privacy and Cyber Security training guidelines.**

6.1.i) Describe how personal information that is shared is transmitted or disclosed. **Printed paper records, viewing of electronic data on computer screen, secure email, facsimile or by telephone.**

6.1.j) Is a Memorandum of Understanding (MOU), contract, or any other agreement in place with all external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared? If an MOU is not in place, is the sharing covered by a routine use in the System of Records Notice? If not, explain the steps being taken to address this omission. **A MOU/ contract/any other agreement is not in place with ALL external organizations. Medical records – YES, sharing is covered by routine use or disclosure under SORN 79VA19, items 22 and 23 and also under 24VA19, item 29. Steps taken - Privacy Officer has obtained a spreadsheet of all contracts for VA MT HCS and identified those that involve use and disclosure of PHI. PO to work with Contracting office to put in place the BAA, MOU or Statement of Work as applicable, in accordance with VA Directive 6066, dated 4/2/2008.**

6.1.k) How is the shared information secured by the recipient? **Contractors and VA staff – Governed by applicable HIPAA and Privacy Laws. If handling paper documents, reasonable precautions are taken to secure the data, such as keeping in locked room, locked area or out of plain sight. When not needed, they are discarded in approved shred containers, and then shredded by contracted company. Electronic data viewed on computers have Privacy filters installed on screens to help obstruct unauthorized viewing. Secured email is used to transmit PHI. Facsimiles are sent to verified users and they exercise reasonable in-house precautions as according to HIPAA. Contractors and staff are advised on Privacy precautions when conducting telephone calls or leaving phone messages.**

6.1.l) What type of training is required for users from agencies outside VA prior to receiving access to the information? **All are required to complete the computer training modules for Cyber Security Training and Web-based Privacy Training prior to receiving access.**

**Section 6.1 Review:**

Privacy Officer has reviewed and approved the responses in this section.

Date of Review: March 19, 2008      2<sup>nd</sup> draft completed: May 8, 2008      3<sup>rd</sup> draft completed May 28, 2008

Privacy Officer: Lesa Wallis (406) 447-7670

**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.)

[http://www1.va.gov/vhapublications/viewpublication.asp?pub\\_id=1089](http://www1.va.gov/vhapublications/viewpublication.asp?pub_id=1089)

YES	The internet site will provide a link that leads to their information. See 6.2.b)
YES	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>
YES	The internet site 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.

**Privacy Impact Assessment 2008 / VISTA  
VA Montana Healthcare System**

6.2.b) What are the procedures that allow individuals to gain access to their own information? **Patients (veterans and CHAMPVA dependents) – Day of Appointment – may view electronic chart and obtain copy of that day’s treatment record, lab result or medication listing for purpose of education and treatment without release of information form. My HealtheVet website – patients may be granted access to certain electronic medical records through this website, after completing in-person authentication process. Patients and VA staff - Requests for access and copies of historical data must be in writing and will be reviewed by Release of Information office with advisement of the appropriate originating department.**

6.2.c) What are the procedures for correcting erroneous information? **Patients must submit a written request to amend, correct or delete information from their records. The Privacy Officer coordinates with the originating department for a review of the request and any actions to be taken. PO sends decision letters to patients and makes the appropriate amendment action, if applicable, to the electronic or paper record. PO coordinates appeal actions for denied requests. Ref: VHA Handbook 1605.1**

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

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

**Section 6.2 Review**

Privacy Officer has reviewed and approved the responses in this section.

Date of Review: March 19, 2008      2<sup>nd</sup> draft completed: May 8, 2008      3<sup>rd</sup> draft completed May 28, 2008

Privacy Officer: Lesa Wallis (406) 447-7670.

**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.  
[http://www1.va.gov/vapubs/viewPublication.asp?Pub\\_ID=19&FTtype=2](http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&FTtype=2)

System of Records Notices may be accessed via: <http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm>  
Or [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)

For VHA projects, VHA Handbook 1907.1 (Section 6j) and VHA Records Control Schedule 10-1 provide more general guidance. [http://vaww1.va.gov/vhapublications/ViewPublication.asp?pub\\_ID=1469](http://vaww1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1469) and VHA Records Control <http://www1.va.gov/vhapublications/RCS10/rcs10-1.pdf>

7.a) What is the data retention period? Given the purpose of retaining the information, explain why the information is needed for the indicated period. **Clinical information is retained in accordance with VA Records Control Schedule 10-1. Demographic information is updated as applications for care are submitted and retained in accordance with VA Records Control Schedule 10-1.**

7.b) What are the procedures for eliminating data at the end of the retention period? **Electronic Final Version of Patient Medical Record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records Control Schedule 10-1, Item XLIII, 2.b. (Page 190). At the present time, VISTA Imaging retains all images.**

7.c) Where are procedures documented? [http://vaww1.va.gov/vapubs/viewPublication.asp?Pub\\_ID=19&FTtype=2](http://vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&FTtype=2) and VHA Records Control <http://www1.va.gov/vhapublications/RCS10/rcs10-1.pdf>

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

**The Health Information Resources Service (HIRS) is responsible for developing policies and procedures for effective and efficient records management throughout VHA. In addition, HIRS acts as the liaison between VHA and National Archives and Records Administration (NARA) on issues pertaining to records management practices and procedures.**

**Chief of Health Information Management is responsible for records management activities at their facilities.**

**Privacy Impact Assessment 2008 / VISTA  
VA Montana Healthcare System**

Program officials are responsible for creating, maintaining protecting, and disposing of records in their program area in accordance with NARA regulations and VA policy.

All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures.

7.e) If applicable, has the retention schedule been approved by the National Archives and Records Administration (NARA)? **Not applicable**

**Section 7 Review:**

Privacy Officer has reviewed and approved the responses in this section.

Date of Review: March 19, 2008 | 2<sup>nd</sup> draft completed: May 8, 2008 | 3<sup>rd</sup> draft completed May 28, 2008

Privacy Officer: Lesa Wallis (406) 447-7670

**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.):

<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.

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.. The VISTA Security Plan is updated periodically to reflect the results of IT security controls adopted for implementation through the annual FISMA Assessment. 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 (ISO) 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. System to undergo certification and accreditation every 3 years. **Monitoring:** Accounting, Audit trail are monitored per the local Center Circular 04C-05-01 currently under revision. **Testing:** security is tested annually per Center Circular 04C-05-01. **Evaluation:** The Center Circular 04C-05-01 is in place to address evaluations that are to be done annually.

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

**8.2 Project-Specific Security Measures**

**Privacy Impact Assessment 2008 / VISTA  
VA Montana Healthcare System**

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

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? **Risks associated with the following conditions: Air Conditioning Failure, Weather, Earthquakes, Theft, Bomb, Communication Loss or Fire hazards.**

8.2.d) Explain what security controls are being used to mitigate these risks. **Controls are consistent with NIST 800-53. Security Controls to mitigate the above mentioned risks are managed by the Regional Data Processing Center located 800 miles away in Denver and not the responsibility of this facility. Our "Read Only Backup System" is locked in the Computer Room and is adequately protected.**

**Section 8 Review:**

Privacy Officer has reviewed and approved the responses in this section.

Date of Review: March 19, 2008      2<sup>nd</sup> draft completed: May 8, 2008      3<sup>rd</sup> draft completed May 28, 2008

Privacy Officer: Lesa Wallis (406) 447-7670

**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 )

N/A

**Section 9 Review:**

**Privacy Impact Assessment 2008 / VISTA  
VA Montana Healthcare System**

Privacy Officer has reviewed and approved the responses in this section.

Date of Review: March 19, 2008      2<sup>nd</sup> draft completed: May 8, 2008      3<sup>rd</sup> draft completed May 28, 2008

Privacy Officer: Lesa Wallis (406) 447-7670

**10. CHILDREN'S ONLINE PRIVACY PROTECTION ACT**

10.a) Will information be collected through the Internet from children under age 13? **NO**

**Section 10 Review:**

Privacy Officer has reviewed and approved the responses in this section.

Date of Review: March 19, 2008      2<sup>nd</sup> draft completed: May 8, 2008      3<sup>rd</sup> draft completed May 28, 2008

Privacy Officer: Lesa Wallis (406) 447-7670

**11. PIA Assessment**

11a) Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA. Examples of choices made include reconsideration of: collection source, collection methods, controls to mitigate misuse of information, provision of consent and privacy notice, and security controls. **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? **Access Control, Audit and Accountability, Identification and Authentication, and System and Communications Protection are in place and 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?

**YES      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.**

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?

**YES      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.**

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?

**YES      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.**

11f) What was the highest impact from questions 11c, 11d, and 11e? **HIGH**

11g) What controls are being considered for this impact level? **Management, Technical, and Operational Controls as outlined in NIST 800-53**

**Section 11 Review:**

Privacy Officer has reviewed and approved the responses in this section.

Date of Review: March 19, 2008      2<sup>nd</sup> draft completed: May 8, 2008      3<sup>rd</sup> draft completed May 28, 2008

Privacy Officer: Lesa Wallis (406) 447-7670

**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

**Privacy Impact Assessment 2008 / VISTA  
VA Montana Healthcare System**

document and, if prepared, summary, are made publicly available (consistent with executive branch policy on the release of information about systems for which funding is proposed).

1. Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment. Such information shall be protected and handled consistent with the Freedom of Information Act (FOIA).

2. Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds.

12.a) Does this PIA contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public? **YES**

12.b) If yes, specify: **Information related to Risk Assessments is considered "Sensitive" therefore request that 8.2 c and 8.2 d be removed from the document prior to its being published.**

**Section 12 Review:**

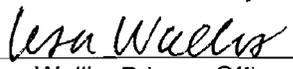
Privacy Officer has reviewed and approved the responses in this section.

Date of Review: March 19, 2008	2 <sup>nd</sup> draft completed: May 8, 2008	3 <sup>rd</sup> draft completed May 28, 2008
--------------------------------	--	--

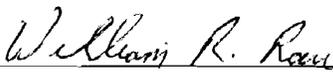
Privacy Officer: Lesa Wallis (406) 447-7670

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

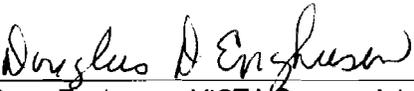
13.1) I have carefully reviewed the responses to each of the questions in this PIA. I am responsible for funding and procuring, developing, and integrating privacy and security controls into the project. I understand that integrating privacy and security considerations into the project may affect the 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.

  
Lesla Wallis, Privacy Officer

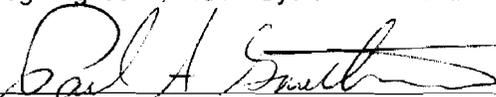
5/28/2008  
Date

  
William Rau, Information Security Officer

5/28/2008  
Date

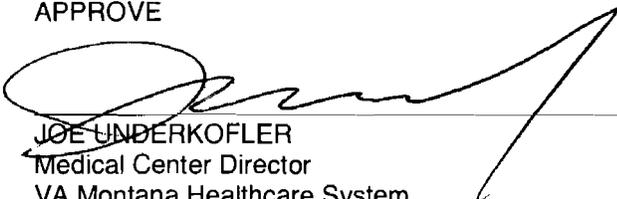
  
Doug Enghusen, VISTA System Administrator

5/28/08  
Date

  
Paul Gauthier, CIO ITS

5/28/08  
Date

APPROVE

  
JOE UNDERKOFLE  
Medical Center Director  
VA Montana Healthcare System