

**Privacy Impact Assessment /VISTA 2008
Grand Junction VAMC**

PRIVACY IMPACT ASSESSMENT 2008	
Part I. Project Identification and Determination of PIA Requirement	
1. PROJECT IDENTIFICATION: VISTA	
1.1) Project Basic Information:	
1.1.a) Project or Application Name:	VISTA Legacy System
1.1.b) OMB Unique Project Identifier:	029-00-01-11-01-1180-00
1.1.c) Concise Project Description	
<p>The VistA Legacy system is comprised of three core platforms:</p> <ol style="list-style-type: none"> 1. InterSystems Cache on VMS [VMS/Cache]. 2. InterSystems Cache on VMS[VMS/Cache] on Linux ECX Shadow server 3. InterSystems Cache on VMS[VMS/Cache] on Linux Servers. <p>Test System consists of a single ES40 server, included are magnetic tape drives (not used), 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) Windows XP throughout the 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.</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: Operational/Maintenance</p>	
1.2) Contact Information:	
1.2.a) Person completing document:	Margaret Grunow
Title:	Privacy Officer
Organization:	Grand Junction VAMC 575
Telephone:	(970) 242-0731 extension 2221
Email Address:	Margaret.Grunow@va.gov
1.2.b) CIO	Craig Frerichs
Title:	Chief Information Officer
Organization:	OI&T/Grand Junction VAMC
Telephone Number:	(970) 256-8908
Email Address:	Craig.Frerichs@va.gov
1.2.C) System Administrator:	Erin Reed
Title:	Vista System Administrator

**Privacy Impact Assessment /VISTA 2008
Grand Junction VAMC**

Organization:	OI&T/Grand Junction VAMC 575
Telephone:	(970) 263-5096
Email Address:	Erin.Reed@va.gov
1.2.d) ISO:	Diana Dillon
Title:	Information Security Officer
Organization:	OI&T/Grand Junction VAMC
Telephone Number:	(970) 263-5013
Email Address:	Diana.Dillon@va.gov
Section 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 personally identifiable verification (PIV) project. A separate PIA has been completed for the PIV project. No PIV information is collected or stored in VISTA	
2.a) Will VISTA collect and/or maintain personally identifiable information of the public in IT systems.	YES
2.b) Is this a PIV project collecting PII, including from Federal employees, contractors, and others performing work for VA? PIV is not collected or maintained on this system.	NA
2.c) Has a previous PIA been completed within the last three years? No	
2.d) Has any changes been made to the system since the last PIA? No	
Section 2 Review:	
Privacy Officer has reviewed and approved the responses in this section.	
Date of Review: November 5, 2008	
Privacy Officer: Margaret Grunow (970) 242 0731 Ext 2221	
Part II Privacy Impact Assessment	
3. Project Description:	
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. Veteran information is collected and stored for the purpose of providing comprehensive health care to our veterans and all business/operation associated with health care.	
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 SOR 23VA163, 24VA19, 97VA105, 99VA13, 121VA19	
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. 52,549 VA personnel and 46,657 patients	
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: November 5, 2008	
Privacy Officer: Margaret Grunow (970) 242 0731 Ext 2221	
4. System 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.b1) Is the system data maintained under one or more approved System(s) of Records? YES	

**Privacy Impact Assessment /VISTA 2008
Grand Junction VAMC**

(1) For each applicable System of Records, list: (1) The System of Records identifier (number). SOR 23VA163, 24VA19, 97VA105, 99VA13, 121VA19	
(2) The name of the System of Records: Veterans Health Information System and Technology Architecture (VISTA-VA), Patient Medical 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/Update_SOR/SOR24VA19.pdf http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf	
4.b.2) Have you read, and will the application comply with, all data management practices in the System of Records? 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.	
4.b.4) Does the System of Records Notice require modification? Modification for this system of Records is NOT Required.	
4.b.5) Describe the required modifications. NONE	
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. NA	
Section 4 Review:	
Privacy Officer has reviewed and approved the responses in this section.	
Date of Review: November 5, 2008	
Privacy Officer: Margaret Grunow (970) 242 0731 Ext 2221	
5. Data Collection:	
5.1 Data Types and Data Uses	
<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>	
YES	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).
NO	Other Personal Information of the Veteran or Primary Subject?
YES	Dependant Information - Demographic, SSN, and Financial information only
YES	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.
Yes	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 veteran patient. Clinical information from VA and DOD is used in the diagnosis and treatment of the veteran.
YES	Criminal Record Information? Criminal information may be flagged

**Privacy Impact Assessment /VISTA 2008
Grand Junction VAMC**

YES	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.
YES	Patient Education information-Education related to the veterans health care
YES	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.
YES	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.
YES	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.
Section 5.1 Review:	
Privacy Officer has reviewed and approved the responses in this section.	
Date of Review: November 5, 2008	
Privacy Officer: Margaret Grunow (970) 242 0731 Ext 2221	
5.2 Data Sources	
<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>	
YES	Veteran Source: Data used to identify the veteran, determine eligibility for care, schedule treatment and manage the provided
NO	Public Sources(s)
YES	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.
YES	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.
YES	State Agency Source(s): Licensing Boards for privileging and credentialing of Providers. Courts for treatment eligibility.
YES	Local Agency Sources (S) Local Hospital, Nursing Homes, Rehabilitation Centers, Hospice, Blood Banks, and Other health care related facilities for coordination of care.
NO	Other Sources(s)

**Privacy Impact Assessment /VISTA 2008
Grand Junction VAMC**

Section 5.2 Review:		
Privacy Officer has reviewed and approved the responses in this section.		
Date of Review: November 5, 2008		
Privacy Officer: Margaret Grunow (970) 242 0731 Ext 2221		
5.3 Collection Methods		
<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.		
YES	Web Forms	Information collected on Web Forms and sent electronically over the Internet to project systems. The web form is located https://www.1010ez.med.va.gov/sec/vha/1010ez/showForm.asp . This form can be printed out, filled out and mailed or taken in to their VA but they are not electronically sent.
YES	Paper Forms	Information collected on Paper Forms and submitted personally, submitted via Postal Mail and/or submitted via Fax Machine. VA Form 1010EZ
YES	Electronic File Transfer (shared)	Information stored on one computer/system (not entered via a Web Form) and transferred electronically to VISTA. 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 Information is shared (not transferred to other systems) within VA, for the purpose of payroll processing, financial and budget related information, workload and performance indicators.
YES	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.
YES	Telephone Contact	Information is collected via telephone. Veterans may answer questions posed over phone to collect Form 1010EZ data, as part of the annual update but the first time they in enroll, they will have to sign the 1010 EZ indicating understanding of the privacy statement and authorizing us to provide health care.
NO	Other Collection Method	Information is collected through a method other than those listed above.
Section 5.3 Review:		
Privacy Officer has reviewed and approved the responses in this section.		
Date of Review: November 5, 2008		
Privacy Officer: Margaret Grunow (970) 242 0731 Ext 2221		
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		

**Privacy Impact Assessment /VISTA 2008
Grand Junction VAMC**

5.4.b) Is the data collection mandatory or voluntary? Voluntary		
5.4.c) How are the individuals involved in the information collection notified of the Privacy Policy and whether provision of the information is mandatory or voluntary? Privacy information is provided in Section V or the VA Form 1010EZ , this is the form that is used to apply for enrollment in the VA health care system.		
5.4.d) Is the data collection new or ongoing? Ongoing		
5.4e.1) If personally identifiable information is collected online, is a privacy notice provided that includes the following elements? Information is not collected online		
NO	Not applicable	
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")		
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.		
<i>Note: if PII is transferred from other projects, explain any agreements or understandings regarding notification of subjects</i>		
Privacy Statement from Section V of the 1010EZ		
Privacy Act Information: VA is asking you to provide the information on this form under 38 U.S.C. Sections 1705,1710, 1712, and 1722 in order for VA to determine your eligibility for medical benefits. Information you supply may be verified through a computer-matching program. VA may disclose the information that you put on the form as permitted by law. VA may make a "routine use" disclosure of the information as outlined in the Privacy Act systems of records notices and in accordance with the VHA Notice of Privacy Practices. You do not have to provide the information to VA, but if you don't, VA may be unable to process your request and serve your medical needs. Failure to furnish the information will not have any affect on any other benefits to which you may be entitled. If you provide VA your Social Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law. Additional Privacy information can be obtained at: http://www.va.gov/privacy		
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. Privacy Notice is in Section V (above) These are not sent electronically.
YES	Paper Forms:	Patients fill out required fields of information on Form 1010 and an explanation of privacy policy provided. Privacy Notice is in Section V (above)
YES	Electronic File Transfer:	Information input at this facility is stored in the VISTA system located at the Regional Data Center in Denver. This information is used in providing veteran healthcare and Business Operations, i.e. Billing and collection. The same is true of the EKG/Cardiology information stored on the MUSE system in the RDPC. PACS (VISTA Imaging) interfaces with VISTA but the images are stored on the PACs Servers here. VISTA Imaging information is shared with 2 of local hospitals via VPN Faxes, with PII, may be sent if coordinating care with an outside provider. There is no separate Privacy information provided for this activity as it is covered by the Privacy Act Information shown above (from the 1010 EZ) and patient has concurred with his/her signature.
YES	Computer Transfer Device:	Additional/separate Privacy information is not provided. We do not sell, rent, or otherwise provide your personal information to outside marketers. Information collected from the VA Form 10-10 EZ may be shared with employees, contractors, and other service providers as necessary to respond to a request, provide a service, or as otherwise authorized by law. There is no personal information collected from the web.
YES	Telephone	Initial 10-10 EZ information is not taken over the phone by this facility. After the veteran has enrolled, his annual update may be handled over the phone. This is after he has reviewed the privacy statement shown above and showed his concurrence by signing the form.
NO	Other Method:	NA
Section 5.4 Review:		
Privacy Officer has reviewed and approved the responses in this section.		
Date of Review: November 5, 2008		
Privacy Officer: Margaret Grunow (970) 242 0731 Ext 2221		

Privacy Impact Assessment /VISTA 2008 Grand Junction VAMC

5.5 Consent for Secondary Use of PII:		
<p><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></p> <p>We do not sell, rent, or otherwise provide your personal information to outside marketers. Information collected via VA Form 10-10 EZ may be shared with employees, contractors, and other service providers as necessary to respond to a request, provide a service, or as otherwise authorized by law.</p>		
<p>5.5.a) Will personally identifiable information be used for any secondary purpose? A release is signed with the 10-10 EZ that allows sharing of information for the purpose of determining eligibility, providing health care, or billing. Otherwise as directed by Federal or State Law. <i>See 5.4 f a</i></p> <p>Title 38 USC 5701 allows release of personal information to civil law enforcement. Additional release is not required.</p> <p>Colorado State Statue 25-1.5-102 requires contagious diseases be reported to public health. Included in this disclosure would be the name and the condition of the patient. Additional release is not required</p> <p>In accordance with HIPAA, VA Directive 6502 and VHA Handbook 1605.1 Individually-identifiable information, excluding 38 U.S.C. 7332-protected information, may be disclosed to officials of any criminal or civil law enforcement governmental agency or any official instrumentality charged under applicable law with the protection of public health or safety in response to standing written request letters. These law enforcement agencies are charged with the protection of public safety and the implementation of reporting laws of a State which seek reports on the identities of individuals whom VA has treated or evaluated for certain illnesses, injuries, or conditions. Additional release is not required, however notification is made to individual regarding this disclosure.</p>		
<p>5.5.b) Describe and justify any secondary uses of personal information. Personal information is not used for anything other than what is permitted or required by law.</p>		
<p>5.5.c) For each collection method identified in question 5.3, "Collection Method," describe:</p>		
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. Privacy Notice is in Section V (above) These are not sent electronically. Information is voluntary. To decline the individual would not sign the VA Form 10-10 EZ.
YES	Paper Forms:	Patients fill out required fields of information on Form 1010 EZ and an explanation of privacy policy provided. Privacy Notice is in Section V (above) Information is voluntary. To decline the individual would not sign the VA Form 10-10 EZ.
YES	Electronic File Transfer:	<p>Information input at this facility is stored in the VISTA system located at the Regional Data Center in Denver. This information is used in providing veteran healthcare and Business Operations, i.e. Billing and collection.</p> <p>The same is true of the EKG/Cardiology information stored on the MUSE system in the RDPC. PACS (VISTA Imaging) interfaces with VISTA but the images are stored on the PACs Servers here. VISTA Imaging information is shared with 2 of local hospitals via VPN</p> <p>Faxes, with PII, may be sent if coordinating care with an outside provider.</p> <p>There is no separate Privacy information provided for this activity as it is covered by the Privacy Act Information shown above (VA FORM 10-10EZ) and patient has concurred with his/her signature. To decline the individual would not sign the VA Form 10-10 EZ.</p>
YES	Computer Transfer Device:	Additional/separate Privacy information is not provided. We do not sell, rent, or otherwise provide your personal information to outside marketers. Information collected from the VA Form 10-10 EZ may be shared with employees, contractors, and other service providers as necessary to respond to a request, provide a service, or as otherwise authorized by law. There is no personal information collected from the web.
YES	Telephone	Initial 10-10 EZ information is not taken over the phone by this facility. After the veteran has enrolled, his annual update may be handled over the phone. This is after he has reviewed the privacy statement shown above and showed his concurrence by signing the form. Information is voluntary. To decline the individual would not sign the VA Form 10-10 EZ.
Note: If you have selected No above, then SKIP to question 5.6, "Data Quality."		
Section 5.5 Review:		
Privacy Officer has reviewed and approved the responses in this section.		
Date of Review: November 5, 2008		

**Privacy Impact Assessment /VISTA 2008
Grand Junction VAMC**

Privacy Officer: Margaret Grunow (970) 242 0731 Ext 2221	
5.6 Date Quality	
5.6.a) Explain how collected data are limited to required elements: When information is shared with authorized Service or Agency information is limited to the elements required.	
5.6.b) How is data checked for completeness? Data is reviewed by staff and compared to source information. System checks are in place for required information and reports provide user with information on deficiencies.	
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 verified each time the individuals come for care or if not seen within the year, the information will be reviewed annually.	
5.6.d) How is new data verified for relevance, authenticity and accuracy? New data is verified with the individual providing the information.	
Section 5.6 Review:	
Privacy Officer has reviewed and approved the responses in this section.	
Date of Review: November 5, 2008	
Privacy Officer: Margaret Grunow (970) 242 0731 Ext 2221	
6. Use and Disclosure	
6.1 User Access and Data Sharing	
Identify the individuals and organizations that have access to system data.	
--> Individuals - Access granted to individuals should be limited to the data needed to perform their assigned duties. Individuals with access to personal information stored in project system must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to prevent as well as detect unauthorized access and browsing.	
--> Other Agencies – Any Federal, State or local agencies that have authorized access to collected personal information must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to protect personal information.	
--> Other Systems – Information systems of other programs or projects that interface with the information system(s) of this project must be identified and the transferred data must be defined. Also, the controls that are in place to ensure that only the defined data are transmitted must be defined.	
6.1.a) Identify all individuals and organizations that will have access to collected information. Select all applicable items below.	
YES	System Users
YES	System Owner: Region One RDPC is owner of the equipment and OI&T has Admin rights
YES	System Administrator
YES	Contractor and Fee for Service Physicians, 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. (Specialty Contracts such as Urology, Orthopedics, Ophthalmology, Cardiology to name a few)
NO	Other Veteran Organization
YES	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. In addition, certain clinical information is being shared with Public Health, also under an established Data Use Agreement (DUA). By law, we are required to report certain conditions/diseases to Public Health, the State Department of Health. We also work with the IRS in determining eligibility and billing, and Medicare (MRA).
YES	State Government Agency – State Health Association – by law
NO	Local Government Agency
NO	Other Projects/Systems
YES	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

**Privacy Impact Assessment /VISTA 2008
Grand Junction VAMC**

	in effect for over three years. In addition, certain clinical information is being shared with Public Health, also under an established DUA.
	<i>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</i>
	6.1.a.1) Describe here who has access to personal information maintained in facility's IT systems: Clinical and administrative personnel involved in the providing or billing for health care.
	6.1.b) How is access to the data determined? Access is given based on the requirements of the job being done. Restricted by role
	6.1.c) Are criteria, procedures, controls, and responsibilities regarding access documented? If so, identify the documents. YES-VA Directive 6502,VHA Directive1605.1 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. Restricted - Menu assignments are restricted by role. Menus reflect what is required to do the job assigned.
	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) Identification and authentication Restricted access based on role Separation of Duties Session Lock after 15 minutes inactivity Session Termination Security Awareness Training Continuous Monitoring New password required every 90 days Strong password required Physical Environment Visitor Control Media Sanitation and Disposal Patch Management Personnel Screening
	6.1.f) Is personal information shared (is access provided to anyone other than the system users, system owner, Project Manager, System Administrator)? Yes information is shared where required by law.
	6.1.g) Identify the measures taken to protect the privacy right of the individuals whose data will be shared. If emailed, it is encrypted. If information is being taken directly from our systems, there systems will be at least as secure as ours.
	6.1.h) Identify who is responsible, once personal information leaves your project's IT system, for ensuring that the information is protected. We are responsible until it is in the possession of the party requiring the information.
	6.1.j) Is a Memorandum of Understanding (MOU), contract, or any other agreement in place with all external organization with whom information is shared? If not, explain the steps being taken to address this omission. Memorandum of Understanding are in place and managed at a National level, not a facility level.
	6.1.k) How is the shared information secured by the recipient? Agencies that information is shared with are covered by the same or similar laws for protecting information that we have.
	6.1.i) What type of training is required for users from agencies outside VA prior to receiving access to information? Federal Agencies all fall under OMB – A-130 requires all employees to take at least 1 hour of privacy and computer security training annually.
	Note: If you have selected No above, then SKIP to question 6.2, "Access to Records and Requests for Corrections".
	Section 6.1 Review:
	Privacy Officer has reviewed and approved the responses in this section.
	Date of Review: November 5, 2008
	Privacy Officer: Margaret Grunow (970) 242 0731 Ext 2221
	6.2 Access to Records and Requests for Corrections
	<i>The Privacy Act and VA policy provide certain rights and mechanisms by which individuals may request</i>

**Privacy Impact Assessment /VISTA 2008
Grand Junction VAMC**

<i>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.) 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. http://www1.va.gov/vhapublications/viewpublication.asp?pub_id=1089
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.
6.2.b) What are the procedures that allow individuals to gain access to their own information? Individuals wishing to access information from their health record can go to the VAMC, Release of Information office (ROI), complete SF-10-5345a and the information will be provided to them. For more information call (970) 242 0731 extension 12204. Requested information will be available within 20 days. Delivery method will have been determined in the request.	
6.2.c) What are the procedures for correcting erroneous information? Veteran must submit the request in writing. Adequately describe the specific information the individual believes to be inaccurate, incomplete irrelevant, or untimely and the reason for this belief. Request must be sent to the Privacy Officer of VAMC where the records are maintained. It will be reviewed and if approved by management, the corrections will be made. Individual will receive copy of amended record or reason for denial and provided with their appeal rights.	
6.2.d) If no redress is provided, are alternatives available? NA	
6.2.e) Provide here any additional explanation; if exempt, explain why the application is exempt from providing access and amendment. The patient is mailed a notice describing the process.	
Section 6.2 Review:	
Privacy Officer has reviewed and approved the responses in this section.	
Date of Review: November 5, 2008	
Privacy Officer: Margaret Grunow (970) 242 0731 Ext 2221	
7. Retention and Disposal	
<i>By completing this section, you provide documented assurance that proper data retention and disposal practices are in place.</i>	
<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>	
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	
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	
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 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 patient care information.	

**Privacy Impact Assessment /VISTA 2008
Grand Junction VAMC**

7.c) <i>Where are procedures documented?</i> VA Handbook 6300.01 at: http://vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&FTYPE=2 and VHA Records Control http://www1.va.gov/vhapublications/RCS10/rcs10-1.pdf
7.d) <i>How are data retention procedures enforced?</i> Retention: Electronically stored information is being retained. All Records – Retained in accordance VHA Records Control Schedule 10-1, VA Handbook 6300.1 Medical Records are pulled from shelf 1 year after death or 3 years of inactivity sent to the Federal Records Center in Neosho, WI Health Information Management Service (HIMS) is responsible for Records Management at this facility.
7.e.) IF applicable, has the retention schedule been approved by the National Archives and Records Administration (NARA). Yes March 31, 2008
Section 7 Review:
Privacy Officer has reviewed and approved the responses in this section.
Date of Review: November 5, 2008
Privacy Officer: Margaret Grunow (970) 242 0731 Ext 2221
8. SECURITY (REMOVED – SENSITIVE INFORMATION)
9. Change Record
<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 <i>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). first PIA</i>
<i>If no, then proceed to Section 10, “Children’s Online Privacy Protection Act.”</i>
Section 9 Review:
Privacy Officer has reviewed and approved the responses in this section.
Date of Review: November 5, 2008
Privacy Officer: Margaret Grunow (970) 242 0731 Ext 2221
10. Children’s Online Privacy Protection Act
10.a) <i>Will information be collected through the Internet from children under age 13?</i> NO
<i>If “No” then Skip to Section 11, “PIA Considerations”.</i>
Section 10 Review:
Privacy Officer has reviewed and approved the responses in this section.
Date of Review: November 5, 2008
Privacy Officer: Margaret Grunow (970) 242 0731 Ext 2221
11. PIA Assessment
11a) <i>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.</i> 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) <i>What auditing measures and technical safeguards are in place to prevent misuse of data?</i> Audits such as Sensitive Record Review, Last Log On, User Failed Access Attempts, Sign-on log, Display user access to patient record, 90 day VISTA Menu Review, User Audit Display, List user holding certain keys, Option access by user and Access File Review and Master Training Report.

**Privacy Impact Assessment /VISTA 2008
Grand Junction VAMC**

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 <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?	
YES	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?	
YES	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.
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: November 5, 2008	
Privacy Officer: Margaret Grunow (970) 242 0731 Ext 2221	
12. PUBLIC AVAILABILITY	
<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 assessment⁹. 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? Yes, Information related to the Risk Analysis is considered "Sensitive". Information in 8.2.c and 8.2 d should not be included in public disclosure.	
Section 12 Review:	
Privacy Officer has reviewed and approved the responses in this section.	
Date of Review: November 5, 2008	
Privacy Officer: Margaret Grunow (970) 242 0731 Ext 2221	

Privacy Impact Assessment /VISTA 2008
Grand Junction 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.



Craig Prerichs
Chief Information Officer
OI&T, Grand Junction, CO

June 10, 2008

Date