

Welcome to the PIA for FY 2012!	
Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.	Macros Must Be Enabled To Use Full Functionality For This Form Template!
	Microsoft Office 2003: To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on <u>Enable Macros at the prompt.</u> Or 1) When file opens click on <u>Enable Macros at the prompt.</u>
To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.	Microsoft Office 2007: To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable All Macros; 2) Click OK
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.	Final Signatures
	Final signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.
Directions:	Privacy Impact Assessment Uploaded into SMART
VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program. If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.	All PIA Validation Letters should be mailed to Christina.Pettit@va.gov to receive full credit for submission.
INTERNAL WEBSITE : http://vawww.privacy.va.gov/PIA.asp	Various Privacy Data Websites:
EXTERNAL WEBSITE : http://www.privacy.va.gov/PRIVACY/Privacy_Impact_Assessment.asp	SORNS : http://www.rms.oit.va.gov/SOR_Records.asp
	Directive Itself (6508): http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=414&FTType=2
Roles and Responsibilities:	Schedule FY 2012 : http://www.privacy.va.gov/PRIVACY/Privacy_Impact_Assessment.asp
Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 referenced in the procedure section of this document.	
a. Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Directive 6508	
b. Records Officer is responsible for supplying records retention and deletion schedules	
c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Directive 6508 and to immediately report all anomalies to the Privacy Service and appropriate management chain.	
d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.	
e. Chief Information Officer (CIO) is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.	
Definition of PII (Personally Identifiable Information)	
Personally Identifiable Information (PII) is —any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.	
Examples of PII include, but are not limited to:	
• Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card	
• Address information, such as street address or email address	
• Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)	
• Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).	
Organizations should minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission.	
A "routine use" is a Privacy Act discretionary authority published in the Federal Register that permits VA to disclose information or records from a Privacy Act-protected record without the patient's prior signed authorization. A "routine use" permits the:	
(1) Release of PHI only when disclosure is also authorized by other applicable legal authorities, including 45 CFR Parts 160 and 164;	
(2) Release of drug or alcohol abuse, HIV, or sickle cell anemia medical information only when the disclosure is also authorized by 38 U.S.C. 7332.	

(FY 2012) PIA: System Information		*Green Highlight = Must Answer Question		*Yellow Highlight = Required to Sign PIA	
Program or System Name (as shown in SMART):		REGION 3>VHA>VISN10>CINCLINNATI VAMC>VISTA - VMS			
OMB Unique System / Application / Program Identifier (AKA: UPID #):		029-00-01-11-01-1180-00			
Description of System/ Application/ Program : "must match what is stated in System Security Plan (SSP)" ***Do not type more than allotted space!!!***		The Vista-Legacy system is the software platform and hardware infrastructure (associated with clinical operations) on which the VHA health care facilities operate their software applications and support for E-Government initiatives. It includes the computer equipment associated with clinical operations and the employees (approx 2500 FTE) necessary to operate the system. Vista - Legacy is a client-server system that links the facility computer network to over 100 applications and databases.			
Facility or Program Office Name:					
Title:	Name:	Phone:	Email:		
Privacy Officer:	Anthony Martin	513-861-3100 x6023	Anthony.Martin@va.gov		
Information Security Officer:	Anita Feiertag	513-475-6590	Anita.Feiertag@va.gov		
System Owner/Delegate:	Michael E. Lay	734-222-4333	Michael.Lay@va.gov		
Chief Information Officer:	Vique Caro	513-861-3100 x6555	Vique.Caro@va.gov		
Information Owner:	Linda Smith	513-861-3100 x6300	LindaD.Smith@va.gov		
Vista Systems Manager	Gary Haney	513-861-300 x4566	Gary.Haney@va.gov		
Person Completing Document:	Aaron Fogle	513-475-6913	Aaron.Fogle@va.gov		
Other Titles:					
Date of Last Full Approved PIA by VACO Privacy Services: (MM/YYYY)		07/2009			
What specific legal authorities authorize this program or system:		Title 38, US Code, Section 7301(a)			
What is the expected number of individuals that will have their PII stored in this system:		1,000,000 -9,999,999			
Identify what stage the System / Application / Program is at:		Operations/Maintenance			
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.		Approx 27 years			
Is there an authorized change control process which documents any changes to existing applications or systems?		<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PIA			
If No, (Explain on Tab 8)					
Is there a contingency plan in place to process information when the system is down?		<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PIA			
Has a PIA been completed within the last three years?		<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PIA			
FISMA QUESTIONS					
1. Is this a new system?		<input type="radio"/> Yes <input checked="" type="radio"/> No			
2. Does this system contain Federal information in identifiable form?		<input checked="" type="radio"/> Yes <input type="radio"/> No			
3. Does the system include information on the public?		<input checked="" type="radio"/> Yes <input type="radio"/> No			
4. System information		<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> National Security System under 40 U.S.C. 11103, a PIA is not required for this system			

5. Is Federal-owned information in this system retrieved by name or unique	<input checked="" type="radio"/> Yes <input type="radio"/> No			
6. What is the System of Records Notice (SORN) for this system?	79VA19			
7. Has this SORN been reviewed or updated within the last three years?	Yes two years ago			
Date of Report (MM/YYYY):			14-Jun-12	
Any check mark in the boxes below will require a full PIA. Please continue to the next TAB and complete the remaining questions.				
If there is no Personally Identifiable Information on your system , please complete TAB 2 & TAB 12. (See Comment for Definition of PII)				
<input type="checkbox"/> Have any changes been made to the system since the last PIA?				
<input type="checkbox"/> Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?				
<input checked="" type="checkbox"/> Will this system/application/program retrieve information on the basis of name, unique identifier, symbol or other PII data?				
<input checked="" type="checkbox"/> Does this system/application/program collect, store, or disseminate PII/PHI data?				
<input checked="" type="checkbox"/> Does this system/application/program collect, store or disseminate the SSN?				
Directions				

(FY 2012) PIA: System of Records

*Green Highlight = Must Answer Question

- 1. Is a SORN (System of Records Notice) Required?
- 2. Is there a SORN already in place?

Yes No Not Sure

Yes No

***If Yes, select all of the appropriate SORN number(s):
 ***If Not Sure, continue to question 3

***Click to add. Delete SORN by highlighting SORN and comma if included and press the Delete key or place focus on area to delete all SORNs.

LIST OF SORN NUMBER(S) :

79VA19

For each applicable System(s) of Records, list:

- 3. If records are retrieved using any of the following entities, A SORN will be required (Please check all that apply)

<input checked="" type="checkbox"/> Full Name
<input checked="" type="checkbox"/> Maiden Name
<input type="checkbox"/> Mother's Maiden Name
<input checked="" type="checkbox"/> Alias
<input checked="" type="checkbox"/> Social Security Number
<input type="checkbox"/> Passport Number
<input type="checkbox"/> Driver's License Number
<input type="checkbox"/> Taxpayer Identification Number
<input type="checkbox"/> Financial Account Number
<input type="checkbox"/> Credit Card Number
<input type="checkbox"/> Street Address
<input type="checkbox"/> Email Address
<input type="checkbox"/> Photographic Image
<input type="checkbox"/> Fingerprints
<input type="checkbox"/> Handwriting
<input type="checkbox"/> Other Biometric Data
<input type="checkbox"/> Other (Explain on Tab 8)

- 4. Based on Question 3, is a SORN required?

Yes No

Yes No

***If Yes, has the process begun to obtain/acquire a SORN

Location where the specific applicable System of Records Notice may be accessed:

http://www.rms.oit.va.gov/SOR_Records.asp

(FY 2012) PIA: Data Collection And Storage

*Green Highlight = Must Answer Question

Please fill in each column for the data types selected.

Data Type	Collection Method	What are the subjects told about the intended use of their information?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Paper	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 info, SSA and IRS data), enter NOK and emergency contact information and collect insurance information.	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	Paper	Dependent data is utilized to determine eligibility for VA benefits. In addition, NOK	Written	Written
Service Information	Electronic/File Transfer	Military Service Information (Branch of Service)	Verbal	Written
Medical Information	Verbal	Vista-Legacy applications meet a wide range of health care data needs. The Vista-Legacy system operates in medical centers, ambulatory and community-based clinics, nursing homes and domiciliary and thus 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.	Verbal	Written
Criminal Record Information	Electronic/File Transfer	Specific information is not input into the Vista system but the fugitive felon program includes a flag on the patient file identifying the need to contact the VA police.	Verbal/Automatic	Written

Guardian Information	Verbal	Guardian information is often flagged in the medical record to ensure the timely and appropriate notification during healthcare decision making from provider/patient/guardian.	Written	Written
Education Information	N/A			
Benefit Information	Electronic/File Transfer	VIS, HINQ, VERA, KLF used to verify service dates, eligibility, SSN, etc.	Written	Written
Other (Explain on Tab 8)	Paper	Next-of-kin information and emergency contact information, such as name and telephone number, is collected from the veteran to use contact other individuals in case of emergency. In addition, insurance and employment information is available on the veteran for use in billing for care. Religious information is collected to provide for spiritual needs if requested by the veteran.	Written	Written
Data Type	Storage Method	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input type="radio"/> Voluntary	
Family Relation (spouse, children, parents, grandparents, etc)	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input type="radio"/> Voluntary	
Service Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	VA Files/Databases (Identify File)	<input type="radio"/> Mandatory <input type="radio"/> Voluntary	
Medical Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input type="radio"/> Voluntary	
Criminal Record Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	State Agency (Identify)	<input type="radio"/> Mandatory <input type="radio"/> Voluntary	
Guardian Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input type="radio"/> Voluntary	
Education Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input type="radio"/> Voluntary	
Benefit Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	VA Files/Databases (Identify File)	<input type="radio"/> Mandatory <input type="radio"/> Voluntary	
Other (Explain on Tab 8)	<input checked="" type="radio"/> Yes <input type="radio"/> No		<input type="radio"/> Mandatory <input type="radio"/> Voluntary	
	<i>(Please Select Yes/No)</i>			
Proximity and Timing: Is the privacy notice provided at the time of data collection?	<input checked="" type="radio"/> Yes <input type="radio"/> No			
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	<input checked="" type="radio"/> Yes <input type="radio"/> No			
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	<input checked="" type="radio"/> Yes <input type="radio"/> No			
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	<input checked="" type="radio"/> Yes <input type="radio"/> No			
	routine use(s)			

(FY 2012) PIA: Data Sharing *Green Highlight = Must Answer Question	** Any connection external to VA requires an ISA/MOU per VA 6500. This section below must be consistent with your System Security Plan Interconnection Security Agreement section.					
Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing	Is PII or PHI Shared?	What is the procedure you reference for the release of information?	
Internal Sharing: VA Organization	VBA	<input checked="" type="radio"/> Yes <input type="radio"/> No	Healthcare	<input type="radio"/> Yes <input checked="" type="radio"/> No	MCM 00-29	
Other Veteran Organization	Office of Regional Counsel	<input type="radio"/> Yes <input checked="" type="radio"/> No	Other (Explain in Tab 8)	<input type="radio"/> Yes <input checked="" type="radio"/> No	BAA	
Other Federal Government Agency	Congressional Offices	<input type="radio"/> Yes <input checked="" type="radio"/> No	Healthcare	<input type="radio"/> Yes <input checked="" type="radio"/> No	ROI 001B-17	
State Government Agency	CDC	<input type="radio"/> Yes <input checked="" type="radio"/> No	Healthcare	<input type="radio"/> Yes <input checked="" type="radio"/> No	DTA	
Local Government Agency	N/A	<input type="radio"/> Yes <input checked="" type="radio"/> No	N/A	<input type="radio"/> Yes <input checked="" type="radio"/> No	N/A	
Research Entity	Affiliates	<input type="radio"/> Yes <input checked="" type="radio"/> No	Healthcare	<input type="radio"/> Yes <input checked="" type="radio"/> No	HIPAA Authorization/Waiver	
<input type="checkbox"/> Other Project/ System (Explain on Tab 8)						
(FY 2012) PIA: Access to Records						
Does the system gather information from another system?		<input checked="" type="radio"/> Yes <input type="radio"/> No				
Please enter the name of the system:		Regional Office - HINQ. It sends information through Vista e-mail. VHA - HEC share eligibility data.				
(FY 2012) PIA: Secondary Use						
Will PII data be included with any secondary use request?		<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="checkbox"/> Mental Health	<input type="checkbox"/> HIV	<input type="checkbox"/> Drug/Alcohol Counseling	
Check all that apply		<input type="checkbox"/> Sickle Cell	<input type="checkbox"/> Other (Explain on Tab 8)	<input type="checkbox"/> Research		

(FY 2012) PIA: Records Management		*Green Highlight = Must Answer Question	
Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?			
<input type="radio"/> Yes (Explain on Tab 8) <input checked="" type="radio"/> No			
Is the data collected to only what is necessary to provide requested service?			
<input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8)			
Has the data provided been verified as complete?			
<input checked="" type="checkbox"/> Veteran Verified <input type="checkbox"/> Received From Database <input type="checkbox"/> Verification Unknown			
(FY 2012) PIA: Retention & Disposal			
What is the data retention period?		RCS 10-1 link for VHA: www.va.gov/vhapublications/rcs10/rcs10-1.pdf	
Answer: 75 years		RCS VB-1, Part II Revised for VBA: www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/part2.pdf	
		National Archives and Records Administration: www.nara.gov	
Explain why the information is needed for the indicated retention period?			
Answer: Retention periods for data vary according to type of record. Data owners are responsible for ensuring they follow the			
What are the procedures for eliminating data at the end of the retention period?			
Answer: Electronic Final Version of Patient Medical Record is destroyed/deleted 75 years after the last episode of patient care as			
Where are these procedures documented?			
Answer: Record Control Schedule 10-1			
How are data retention procedures enforced?			
Answer: Program officials are responsible for creating, maintaining, protecting, and disposing of records in their program area in			
Has the retention schedule been approved by the National Archives and Records Administration (NARA)			
<input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8)			
(FY 2012) PIA: Children's Online Privacy Protection Act (COPPA)			
Will information be collected through the internet from children under age 13?			
<input type="radio"/> Yes (Explain on Tab 8) <input checked="" type="radio"/> No			

(FY 2012) PIA: Security *Green Highlight = Must Answer Question

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Is security monitoring conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Is security assessment conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Is adequate physical security in place to protect against unauthorized access?	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)

*Ensure PE 2, PE-3, PE-6, PE-7, PE-8 have been addressed appropriately for your categorization

Explain what security risks were identified in the security assessment? (Check all that apply)

<input type="checkbox"/> Biological Release	<input checked="" type="checkbox"/> Fire	<input checked="" type="checkbox"/> Lightning Strike	<input checked="" type="checkbox"/> Terrorist
<input checked="" type="checkbox"/> Blizzard	<input checked="" type="checkbox"/> Flood	<input checked="" type="checkbox"/> Malicious Code	<input checked="" type="checkbox"/> Thunderstorm
<input checked="" type="checkbox"/> Burglary/Break-In	<input checked="" type="checkbox"/> Hacker, Cracker	<input checked="" type="checkbox"/> Password Privacy Negligence	<input checked="" type="checkbox"/> Tornado
<input checked="" type="checkbox"/> Civil Unrest	<input checked="" type="checkbox"/> Hail	<input checked="" type="checkbox"/> Personnel Unavailable	<input type="checkbox"/> Tsunami
<input checked="" type="checkbox"/> Component Failure	<input checked="" type="checkbox"/> HAZMAT Release/Spill	<input checked="" type="checkbox"/> Power Failure	<input checked="" type="checkbox"/> User Negligence
<input type="checkbox"/> Dam Failure	<input checked="" type="checkbox"/> Human Health Emergency	<input checked="" type="checkbox"/> Sabotage	<input checked="" type="checkbox"/> User Sabotage
<input type="checkbox"/> Dust/Debris	<input type="checkbox"/> Hurricane	<input checked="" type="checkbox"/> System Intrusion, Break-Ins	<input checked="" type="checkbox"/> Vibration
<input checked="" type="checkbox"/> Earthquake	<input checked="" type="checkbox"/> HVAC Failure	<input checked="" type="checkbox"/> System Misconfiguration	<input type="checkbox"/> Volcano
<input checked="" type="checkbox"/> Extreme Cold	<input checked="" type="checkbox"/> Indoor Humidity	<input checked="" type="checkbox"/> System Penetration	<input checked="" type="checkbox"/> Water Damage
<input checked="" type="checkbox"/> Extreme Heat	<input type="checkbox"/> Landslide	<input checked="" type="checkbox"/> System Tampering	<input checked="" type="checkbox"/> Winter Weather Hazards

*If any other risks identified, explain in Tab 8

Based upon the risks identified above, Explain what security controls are being used to mitigate these risks. (Check all that apply)

<input checked="" type="checkbox"/> Access Control	<input checked="" type="checkbox"/> Configuration Management	<input checked="" type="checkbox"/> Media Protection	<input checked="" type="checkbox"/> System and Services Acquisition
<input checked="" type="checkbox"/> Audit and Accountability	<input checked="" type="checkbox"/> Contingency Planning	<input checked="" type="checkbox"/> Personnel Security	<input checked="" type="checkbox"/> System and Communication Protection
<input checked="" type="checkbox"/> Awareness and Training	<input checked="" type="checkbox"/> Identification and Authentication	<input checked="" type="checkbox"/> Physical and Environmental Protection	<input checked="" type="checkbox"/> System and Information Integrity
<input checked="" type="checkbox"/> Security Assessment and Authorization	<input checked="" type="checkbox"/> Incident Response	<input checked="" type="checkbox"/> Risk Assessment	<input checked="" type="checkbox"/> Planning
			<input checked="" type="checkbox"/> Maintenance

Answer: (Other Controls) Explain on Tab 8

PIA: PIA Assessment

Based upon NIST 800-60, volume II; List the Information data types chosen as a basis for your FIPS 199 System Categorization.

Answer:

<p><u>Availability Assessment:</u> If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization? (Choose One)</p>	<input checked="" type="checkbox"/> 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. <input type="checkbox"/> The potential impact is moderate if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> The potential impact is low if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
<p><u>Integrity Assessment:</u> If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? (Choose One)</p>	<input checked="" type="checkbox"/> 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. <input type="checkbox"/> The potential impact is moderate if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> The potential impact is low if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.
<p><u>Confidentiality Assessment:</u> If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? (Choose One)</p>	<input checked="" type="checkbox"/> 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. <input type="checkbox"/> The potential impact is moderate if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> The potential impact is low if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments?
 The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

(FY 2012) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

From Tab 5, No. 6 (Counsel): Tort Claims and Legal Processes

(FY 2012) PIA: VISTA Minor Applications N-Z

Which of these are sub-components of your system?							
	National Cemetery Association	x	Pharmacy Data Management	Scanning Exam and Evaluation System	x	VBECs	
	National Drug File	x	Pharmacy National Database	x	Scheduling	x	VDEF
x	National Laboratory Test		Pharmacy Prescription Practice	Security Suite Utility Pack		Vendor - Document Storage Sys	
	NDBI	x	PICIS OR	x	Sentillion	x	Veterans Canteen Web
x	Network Health Exchange	x	Police & Security	x	Shift Change Handoff Tool	x	Veterans Information Solution
	NOAHLINK	x	Problem List		ShoreTel		VHAHUNAPP1
x	NOIS	x	Progress Notes	x	Social Work		VHAHUNFPC1
x	Nursing Service	x	Prosthetics		Stellant	x	VHS & RA Tracking System
	Occurrence Screen	x	Purchase Order Management System		Stentor	x	Visit Tracking
x	Omnicell	x	Pyxis	x	Surgery	x	VISTA RAD
x	Oncology	x	Q-Matic	x	Survey Generator	x	VISTA RO
	Onicord (VLOG)		QMSI Prescription Processing	x	Telecare Record Manager	x	VistALink
	Optifill		Quality Assurance Integration		Temp Trak		VistALink Security
x	Order Entry/ Results Reporting		Quality Improvement Checklist	x	Text Integration Utilities	x	Visual Impairment Service Team ANRV
x	Outpatient Pharmacy		QUASER		Tickler Database	x	Vitria BusinessWare
x	P2000 ROBOT	x	Radiology/ Nuclear Medicine	x	Toolkit		VIXS
x	PACS database		RAFT		TopCon	x	Voluntary Timekeeping
x	Patch Module		RALS		TraceMaster	x	Voluntary Timekeeping National
x	Patient Data Exchange	x	Record Tracking		Tracking Continuing Education		WEB HINQ
	Patient Feedback	x	Registration	x	Traumatic Brain Injury		Whiteboard
	Patient Representative	x	Release of Information - DSSI		Unwinder	x	Women's Health
x	PCE Patient Care Encounter	x	Remote Order/ Entry System	x	Utility Management Rollup	x	Workload and Overtime
	Personal Computer Generated Letters	x	RPC Broker	x	Utilization Review		
x	Pharmacy Benefits Mangement		Run Time Library		VA Conference Room Registration		
			SAGG	x	VA Fileman		
			SAN		VAMedSafe		
Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.							
Name							
Description							
Comments							
Is PII collected by this minor application?							
Does this minor application store PII?							
If yes, where?							
Who has access to this data?							
Name							
Description							
Comments							
Is PII collected by this minor application?							
Does this minor application store PII?							
If yes, where?							
Who has access to this data?							
Name							
Description							
Comments							
Is PII collected by this minor application?							
Does this minor application store PII?							
If yes, where?							
Who has access to this data?							

(FY 2012) PIA: Final Signatures		*Green Highlight = Must Answer Question	
Facility Name:	0		
Title:	Name:	Phone:	Email:
Privacy Officer:	Anthony Martin	513-861-3100 x6023	Anthony.Martin4@va.gov
	7/3/2012		
X Anthony J. Martin	rtag	513-475-6590	Anita.Feiertag@va.gov
Anthony Martin	Lay	734-222-4333	Michael.Lay@va.gov
X Anita M. Feiertag			
Anita Feiertag		513-861-3100 x6555	Vique.Caro@va.gov
^ Vique Caro			
Michael E. Lay		513-861-300 x4566	Gary.Haney@va.gov
v	7/3/2012		
X Gary Haney	14-Jun-12		
Gary Haney	10-01-11-01-1180-00		
	REGION 3>VHA>VISN10>CINCINNATI VAMC>VISTA - VMS		
<p>The Signature Process:</p> <ul style="list-style-type: none"> • Complete the PIA form. • Name the PIA Excel FORM ["FY12-Region # - Facility Name - Facility # -Date(mmdyyyy).xls"] <ul style="list-style-type: none"> • Example: "FY12-Region3-Lexington VAMC-596-10302008.xls" • Submit the completed PIA Excel form to SMART Database. • Fix errors the reviewers sent back, rename the file and submit to SMART Database <ul style="list-style-type: none"> • If no errors, convert form into PDF with Nuance PDF Professional. • Name the PIA PDF form ["FY12-Region #-Facility Name- Facility # -Date(mmdyyyy).xls"] <ul style="list-style-type: none"> • Obtain digital signatures on the "Final Signatures tab" • Submit signed PIA PDF form to the SMART Database. 			

- 1.16 Update buttons from default to non-default
- 1.16 Fix background of buttons to blend in with cells
 - Expand description cell to accommodate for long
- 1.17 descriptions in tab 2
 - Change Name of Tab 10 from Minor Applications A-M to
- 1.17 VISTA Minor Applications A-M