

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 1 > VHA > VISN 20 > Roseburg HCS > VistA			
OMB Unique System / Application / Program Identifier (AKA: UPID #):		Exhibit 300 ID: 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!!!***		<p>The Veterans Health Information Systems and Technology Architecture (VistA) is an enterprise-wide information system built around an electronic health record. VistA has been used throughout the Veterans Affairs (VA) medical system since 1984.</p> <p>VistA supports both ambulatory and inpatient care, and includes a graphical user interface for clinicians known as the Computerized Patient Record System (CPRS), which was released in 1997. In addition, VistA includes computerized order entry, bar code medication administration, electronic prescribing, and clinical guidelines.</p> <p>CPRS provides a client-server interface that allows health care providers to review and update a patient's electronic medical record. This includes the ability to place orders, including those for medications, special procedures, X-rays, nursing interventions, diets, and laboratory tests.</p> <p>The VARHS VistA system has been centralized to, and replicated between, the two Regional datacenters in Denver and Sacramento – with Sacramento normally providing processing support for VARHS. The VARHS VistA system is now fully administered by the Region 1 VistA Management Team.</p>			
Facility or Program Office Name:		VA Roseburg Healthcare System			
Title:		Name:		Phone:	
Privacy Officer:		Richard Weber		541-440-1000 x44561	
Information Security Officer:		Keleen Wright		541-440-3108	
Information Security Officer:		Becky France		541-677-3113	
System Owner/Delegate:		Jim Hall		541-440-1361	
Chief Information Officer:		Jim Hall		541-440-1361	
Information Owner:		Carol Bogedain		541-440-1000 x44208	
Other Titles:					
Person Completing Document:		Jim Hall		541-440-1361	
Other Titles:					
Date of Last Full Approved PIA by VACO Privacy Services: (MM/YYYY)				04/2009	
What specific legal authorities authorize this program or system:		Title 38, United States Code, section 7301(a).			
What is the expected number of individuals that will have their PII stored in this system:		100000			
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.		22 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			
2. System Information					

4. Is there a Privacy Impact Assessment (PIA) that covers this system?	<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 three years ago			
Date of Report (MM/YYYY):			25-Apr-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 checked="" type="checkbox"/>	Have any changes been made to the system since the last PIA?			
<input checked="" 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 checked="" type="checkbox"/> Mother's Maiden Name
<input checked="" type="checkbox"/> Alias
<input checked="" type="checkbox"/> Social Security Number
<input checked="" type="checkbox"/> Passport Number
<input checked="" type="checkbox"/> Driver's License Number
<input checked="" type="checkbox"/> Taxpayer Identification Number
<input checked="" type="checkbox"/> Financial Account Number
<input checked="" type="checkbox"/> Credit Card Number
<input checked="" type="checkbox"/> Street Address
<input checked="" type="checkbox"/> Email Address
<input checked="" type="checkbox"/> Photographic Image
<input checked="" type="checkbox"/> Fingerprints
<input checked="" type="checkbox"/> Handwriting
<input checked="" 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)	ALL	Healthcare	All	All
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Healthcare	All	All
Service Information	ALL	Eligibility	All	All
Medical Information	ALL	Healthcare	All	All
Criminal Record Information	ALL	Eligibility	All	All
Guardian Information	ALL	Healthcare	All	All
Education Information	ALL	Healthcare	All	All
Benefit Information	ALL	Benefits	All	All
Other (Explain on Tab 8)				
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	On The Form
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	On The Form
Service Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input type="radio"/> Voluntary	On The Form
Medical Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input type="radio"/> Voluntary	On The Form
Criminal Record Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input type="radio"/> Voluntary	On The Form
Guardian Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input type="radio"/> Voluntary	On The Form
Education Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary	On The Form
Benefit Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary	On The Form
Other (Explain on Tab 8)	<input type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary	On The Form
	<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/VHA/MPI/HEC	<input checked="" type="radio"/> Yes <input type="radio"/> No	Benefits, Helathcare, and	<input checked="" type="radio"/> Yes <input type="radio"/> No	VHA Handbook 1605.2
Other Veteran Organization	VSO	<input checked="" type="radio"/> Yes <input type="radio"/> No	Patient Eligibility	<input type="radio"/> Yes <input checked="" type="radio"/> No	HIPAA Authorization/Waiver
Other Federal Government Agency	SSA/DoD/DOJ/HHS/OIG	<input checked="" type="radio"/> Yes <input type="radio"/> No	Healthcare	<input type="radio"/> Yes <input checked="" type="radio"/> No	VHA Handbook 1605.2
State Government Agency		<input checked="" type="radio"/> Yes <input type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Local Government Agency		<input checked="" type="radio"/> Yes <input type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Research Entity	USCF/NCIRE/NIH/DoD	<input checked="" type="radio"/> Yes <input type="radio"/> No	Research	<input type="radio"/> Yes <input checked="" type="radio"/> No	Internal
<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:		VA Austin Automation Center Data Warehouse			
(FY 2012) PIA: Secondary Use					
Will PII data be included with any secondary use request?		<input checked="" type="radio"/> Yes <input type="radio"/> No	<input checked="" type="checkbox"/> Mental Health	<input checked="" type="checkbox"/> HIV	<input checked="" type="checkbox"/> Drug/Alcohol Counseling
Check all that apply			<input checked="" type="checkbox"/> Sickle Cell	<input type="checkbox"/> Other (Explain on Tab 8)	<input checked="" 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 checked="" 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	
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?			
Healthcare Research			
What are the procedures for eliminating data at the end of the retention period?			
Aged off of backups			
Where are these procedures documented?			
RCS 10-1			
How are data retention procedures enforced?			
Backup system			
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 checked="" 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 checked="" 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 checked="" type="checkbox"/> Dam Failure	<input checked="" type="checkbox"/> Human Health Emergency	<input checked="" type="checkbox"/> Sabotage	<input checked="" type="checkbox"/> User Sabotage
<input checked="" type="checkbox"/> Dust/Debris	<input checked="" 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 checked="" 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 checked="" 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: Privacy, Medical, and Financial

<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.

There are no interfaces to information systems external to the VA such as a research facility. VARHS IT Operations staff do not manage or support the VistA system used by the Facility, the VARHS VistA system is just one of 32 VistA systems that are centrally operated and supported by OI&T Region 1 staff. The VARHS VistA system itself is a virtual instance that runs on a sophisticated server and database system located in the Regional Data Center (RDP) in Sacramento, California. The recovery VistA system instance for Roseburg is located in the RDP in Denver, Colorado.

- The RDPs that host the Region 1 VistA Systems are operated by the OI&T Region 1 IT Service Support Service Line.
- The VistA system servers, database, and operating system software are all supported by the OI&T Region 1 Business Systems Service Line.
- The VistA system application programs are managed by the OI&T Region 1 Applications Service Line.
- The RDPs are accessed via the Region 1 Wide Area Network (WAN) which is operated by the OI&T Region 1 Infrastructure Service Line.
- The local VARHS IT Operations staff only provides: account management support for the VARHS VistA instance; communications with end-users when the changes to the VistA system are announced by Region 1 staff; end-user assistance with extract reports; hosting of local medical system gateway servers and application servers; and hosting of the read-only Region 1 VistA contingency server;

The VARHS VistA system is accessed primarily through the use of desktop computers connected to the VARHS Local Area Network (LAN). The VARHS LAN connects to the RDPs via the OI&T Region 1 Wide Area Network (WAN). All of the OI&T Region 1 VistA systems are accessible from anywhere on the VA intranet through the use of Telnet, CPRS, or thin client connection.

(FY 2012) PIA: VBA Minor Applications

Which of these are sub-components of your system?		
Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial		Automated Medical Information Exchange II (AIME II)
Agent Orange	BCMA Contingency Machines	Automated Medical Information System (AMIS)290
Appraisal System	Centralized Property Tracking System	Automated Standardized Performance Elements Nationwide (ASPEN)
ASSISTS	Common Security User Manager (CSUM)	Broome Closet
Awards	Compensation and Pension (C&P)	Centralized Accounts Receivable System (CARS)
Baker System	Control of Veterans Records (COVERS)	Committee on Waivers and Compromises (COWC)
	Courseware Delivery System (CDS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)	Dental Records Manager	
	Education Training Website	Compensation & Pension Training Website
C&P Payment System	Electronic Appraisal System	Distribution of Operational Resources (DOOR)
C&P Training Website	Electronic Card System (ECS)	Educational Assistance for Members of the Selected Reserve Program CH 1606
	Electronic Payroll Deduction (EPD)	Electronic Performance Support System (EPSS)
CONDO PUD Builder	Eligibility Verification Report (EVR)	Enterprise Wireless Messaging System (Blackberry)
	Fiduciary Beneficiary System (FBS)	Financial Management Information System (FMI)
EndoSoft	Fiduciary STAR Case Review	Hearing Officer Letters and Reports System (HOLAR)
FOCAS	Financial and Accounting System (FAS)	Inquiry Routing Information System (IRIS)
Inforce	Insurance Unclaimed Liabilities	
INS - BIRLS	Inventory Management System (IMS)	Modern Awards Process Development (MAP-D)
Insurance Online	Interactive Voce Response (IVR)	Personal Computer Generated Letters (PCGL)
Insurance Self Service	LGY Centralized Fax System	Personnel Information Exchange System (PIES)
LGY Home Loans	Loan Service and Claims	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing		Purchase Order Management System (POMS)
MES	Loan Guaranty Training Website	Reinstatement Entitlement Program for Survivors (REAPS)
Mobilization	Mental Health Assistant	Reserve Educational Assistance Program CH 1607
Montgomery GI Bill	National Silent Monitoring (NSM)	RightFax
MUSE	Powerscribe Dictation System	Service Member Records Tracking System
Omnicell	Rating Board Automation 2000 (RBA2000)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Records Locator System	Systematic Technical Accuracy Review (STAR)
RAI/MDS	Remittance Processing System	Training and Performance Support System (TPSS)
Right Now Web	Review of Quality (ROQ)	VA Online Certification of Enrollment (VA-ONCE)
SAHSHA	Search Participant Profile (SPP)	
Script Pro	Spinal Bifida Program Ch 18	VA Reserve Educational Assistance Program
SHARE	State Benefits Reference System	Veterans Assistance Discharge System (VADS)
Sidexis	State of Case/Supplemental (SOC/SSOC)	Veterans Exam Request Info System (VERIS)
Synquest	Telecare Record Manager	Veterans Insurance Claims Tracking and Response System (VICTARS)
VBA Training Academy	VBA Enterprise Messaging System	Veterans Service Representative (VSR) Advisor
Veterans Canteen Web		Vocational Rehabilitation & Employment (VR&E) CH 31
VETSNET Housekeeping	Web Electronic Lender Identification	Web Automated Folder Processing System (WAFPS)
VR&E Training Website		Web Automated Reference Material System (WARMS)
Web LGY		Web Automated Verification of Enrollment
		Web-Enabled Approval Management System (WEAMS)
		Web Service Medical Records (WebSMR)
		Work Study Management System (WSMS)
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 min or application?		
Does this minor application store PII?		
If yes, where?		
Who has access to this data?		
Name		
Description		
Comments		
Is PII collected by this min or application?		
Does this minor application store PII?		
If yes, where?		
Who has access to this data?		
Name		
Description		
Comments		
Is PII collected by this min or application?		
Does this minor application store PII?		
If yes, where?		
Who has access to this data?		

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

Which of these are sub-components of your system?							
X	National Cemetery Association	X	Pharmacy Data Management	X	Scanning Exam and Evaluation System	X	VBECs
X	National Drug File	X	Pharmacy National Database	X	Scheduling	X	VDEF
X	National Laboratory Test	X	Pharmacy Prescription Practice	X	Security Suite Utility Pack	X	Vendor - Document Storage Sys
X	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
X	NOAHLINK	X	Problem List	X	ShoreTel	X	VHAHUNAPP1
X	NOIS	X	Progress Notes	X	Social Work	X	VHAHUNFPC1
X	Nursing Service	X	Prosthetics	X	Stellant	X	VHS & RA Tracking System
X	Occurrence Screen	X	Purchase Order Management System	X	Stentor	X	Visit Tracking
X	Omnicell	X	Pyxis	X	Surgery	X	VISTA RAD
X	Oncology	X	Q-Matic	X	Survey Generator	X	VISTA RO
X	Onicord (VLOG)	X	QMSI Prescription Processing	X	Telecare Record Manager	X	VistALink
X	Optifill	X	Quality Assurance Integration	X	Temp Trak	X	VistALink Security
X	Order Entry/ Results Reporting	X	Quality Improvement Checklist	X	Text Integration Utilities	X	Visual Impairment Service Team ANRV
X	Outpatient Pharmacy	X	QUASER	X	Tickler Database	X	Vitria BusinessWare
X	P2000 ROBOT	X	Radiology/ Nuclear Medicine	X	Toolkit	X	VIXS
X	PACS database	X	RAFT	X	TopCon	X	Voluntary Timekeeping
X	Patch Module	X	RALS	X	TraceMaster	X	Voluntary Timekeeping National
X	Patient Data Exchange	X	Record Tracking	X	Tracking Continuing Education	X	WEB HINQ
X	Patient Feedback	X	Registration	X	Traumatic Brain Injury	X	Whiteboard
X	Patient Representative	X	Release of Information - DSSI	X	Unwinder	X	Women's Health
X	PCE Patient Care Encounter	X	Remote Order/ Entry System	X	Utility Management Rollup	X	Workload and Overtime
X	Personal Computer Generated Letters	X	RPC Broker	X	Utilization Review	X	
X	Pharmacy Benefits Mangement	X	Run Time Library	X	VA Conference Room Registration	X	
		X	SAGG	X	VA Fileman	X	
		X	SAN	X	VAMedSafe	X	
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:	VA Roseburg Healthcare System		
Title:	Name:	Phone:	Email:
Privacy Officer:	Richard Weber	541-440-1000 x44561	richard.weber3@va.gov
Digital Signature Block			
Information Security Officer:	Becky France	541-677-3113	becky.france@va.gov
Digital Signature Block			
System Owner/Delegate:	Jim Hall	541-440-1361	jim.hall@va.gov
Digital Signature Block			
Chief Information Officer:	Jim Hall	541-440-1361	jim.hall@va.gov
Digital Signature Block			
Other Titles:	0	0	0
Digital Signature Block			
Date of Report:	25-Apr-12		
OMB Unique Project Identifier	Exhibit 300 ID: 029-00-01-11-01-1180-00		
Project Name	REGION 1 > VHA > VISN 20 > Roseburg HCS > VistA		
<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(mmdyyy).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(mmdyyy).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