

<u>Welcome to the PIA for FY 2012!</u>		
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&FTYPE=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 number		
• 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 2 > VHA > VISN 23 > Black Hills HCS > LAN			
OMB Unique System / Application / Program Identifier (AKA: UPID #):		029-00-02-00-01-1120-00			
Description of System/ Application/ Program : "must match what is stated in System Security Plan (SSP)"		Each VA facility uses the Local Area Network (LAN) as a General Support System, supporting mission-critical and other systems necessary to conduct day-to-day operations within the Veterans Health Administration. Applications and devices within the LAN support numerous areas, including medical imaging, supply management, decision support, medical research, and education.			
Facility or Program Office Name:		Ft. Meade, SD and Hot Springs, SD making up Black Hills Health Care System (BHHCS)			
Title:		Name:		Phone:	
Privacy Officer:		DanGadomski		605-347-2511x97623	
Information Security Officer:		Katherine Vollmer		605-745-2000x92258	
System Owner/Delegate:		Stan Bush for BK Hack		612-467-1200	
Chief Information Officer:		John Reiffenberger		605-347-7232	
Information Owner:					
Other Titles:					
Person Completing Document:		Sandra Hedtke		701-237-2566	
Other Titles:					
Date of Last Full Approved PIA by VACO Privacy Services: (MM/YYYY)		08/2009			
What specific legal authorities authorize this program or system:		Title 38, United States Code, Sections 501(b) and 304.			
What is the expected number of individuals that will have their PII stored in this system:		1,000,000+			
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.		17 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. 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. What is the System of Records Notice (SORN) for this system?		24VA19			
6. What is the System of Records Notice (SORN) for this system?		24VA19			
7. Has this SORN been reviewed or updated within the last three years?		Yes two years ago			
Date of Report (MM/YYYY):		01/2012			
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 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?					

This and system/application/program collects 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) :

24VA19

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)

Full Name

Maiden Name

Mother's Maiden Name

Alias

Social Security Number

Passport Number

Driver's License Number

Taxpayer Identification Number

Financial Account Number

Credit Card Number

Street Address

Email Address

Photographic Image

Fingerprints

Handwriting

Other Biometric Data

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	ALL	All	All
Family Relation (spouse, children, parents, grandparents, etc)	ALL	ALL	ALL	ALL
Service Information	ALL	ALL	ALL	ALL
Medical Information	ALL	ALL	ALL	ALL
Criminal Record Information	ALL	ALL	ALL	ALL
Guardian Information	ALL	ALL	ALL	ALL
Education Information	ALL	ALL	ALL	ALL
Benefit Information	ALL	ALL	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 checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	Automated
Family Relation (spouse, children, parents, grandparents, etc)	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary	Automated
Service Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	Automated
Medical Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary	Automated
Criminal Record Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary	Automated
Guardian Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	Automated
Education Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary	Automated
Benefit Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary	Automated
Other (Explain on Tab 8)	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	Automated

	<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	Multiple VA Organizations	<input checked="" type="radio"/> Yes <input type="radio"/> No	All	<input checked="" type="radio"/> Yes <input type="radio"/> No	VHA Handbook 1605.2
Other Veteran Organization	VBA	<input checked="" type="radio"/> Yes <input type="radio"/> No	ALL	<input checked="" type="radio"/> Yes <input type="radio"/> No	VHA Handbook 1605.2
Other Federal Government Agency	DoD, SSA, IRS	<input checked="" type="radio"/> Yes <input type="radio"/> No	ALL	<input checked="" type="radio"/> Yes <input type="radio"/> No	VHA Handbook 1605.2
State Government Agency	State of South Dakota Dept of Health/Dept of Social Services	<input type="radio"/> Yes <input checked="" type="radio"/> No	Healthcare	<input type="radio"/> Yes <input checked="" type="radio"/> No	VHA Handbook 1605.2
Local Government Agency		<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Research Entity		<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
<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:		Minneapolis VAMC Vista system, PAID/DFAS			
(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 checked="" type="checkbox"/> Received From Database <input checked="" 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 past the last documented entry. The VA has detailed retention requirements for different kinds of data and images. We follow RCS 10-1, and VHA Handbook 1907.1 (Section 6) and VHA Records Control Schedule 10-1 provide more general guidance.		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: Record retention is necessary for patient care and research.			
What are the procedures for eliminating data at the end of the retention period?			
Answer: The VA has procedures for eliminating stored data when storage devices are disposed of. These procedures are followed when media, both electronic and paper, must be disposed of. The NIST guidelines are followed.			
Where are these procedures documented?			
Answer: Documented in the System Security Plan, per NIST guidelines/ Procedures for data elimination are detailed in the following documents: VA Black Hills LAN System Security Plan, VA Directive 6500, Policy- N23-CIO-005, and VA Black Hills local policy, DIR-07			
How are data retention procedures enforced?			
Answer: Through policy, procedure and audits and disciplinary actions, if necessary			
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 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 type="checkbox"/> Vibration
<input 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:	Access to Care; Population Health Mgmt & Consumer Safety; Health Care Administration; Health Care Delivery Services; Health Care Research and Practitioner; Education; Administrative Management; Financial Management; Human Resource Management; Supply Chain Management; Information and Technology Management
---------	---

<p>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? (Choose One)</p>	<input 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 checked="" 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>Integrity Assessment: 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>Confidentiality Assessment: 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 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 checked="" 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.

(FY 2012) PIA: Minor Applications A-M

Which of these are sub-components of your system?							
1184 Web	x	Citrix	x	Electronic Signature	x	Imaging	
A4P	x	Clinical Case Registries		Embedded Fragment Registry		Incentive Awards	
X		ACCu Care	x	Clinical Data Repository/Health Data Repository	x	ENCORE 2	Incident Reporting
X		ACCU Check	x	Clinical Info Resource Network		ENDSOFT	Income Verification Match
X		ACCU Med		Clinical Monitoring System	x	Engineering	Incomplete Records Tracking
X		Adobe Acrobat	x	Clinical Notes Templates	x	Enrollment Application System	Inpatient Medications
		ADP Planning (PlanMan)	x	Clinical Procedures		Enterprise Terminology Server & VHA Enterprise Terminology Services	Intake/ Output
X		ADT	x	Clinical Reminders		ePROMISE	Integrated Billing
X		Adverse Reaction Tracking		Clippership	x	Equipment/ Turn-in Request	Integrated Patient Funds
X		Agent Cashier		Combat Veteran Outreach	x	Event Capture	Interim Management Support
X		Air Fortress		Committee on Waiver and Compromises		Event Driven Reporting	Inventory Management System
X		ASISTS	x	Consult/ Request Tracking		Extensible Editor	Kernal
X		Authorization/ Subscription		Controlled Correspondence	x	External Peer Review	Kids
		Auto Instrument	x	Controlled Substances		EYECAP	KOWA
X		Auto Replenishment/ Ward Stock		CP&E	x	Fee Based Claims System	Lab Service
X		AUTOCAD	x	CPRS	x	Fee Basis	Laboratory Electronic Data Interchange
		Automated Access Request	x	CPT/ HCPCS Codes		Financial and Accounting System (FAS)	Letterman
X		Automated Info Collection Sys	x	Credentials Tracking	x	Financial Management System (FMS)	Lexicon Utility
X		Automated Lab Instruments		Credit Card Authentication	x	Functional Independence	Library
X		Automated Med Info Exchange	x	Data Innovations	x	Gen. Med. Rec. - I/O	List Manager
		Automated Sales Reporting		DELIVEREX	x	Gen. Med. Rec. - Vitals	Lynx Duress Alarm
		AutoMed	x	Dental		Gen. Med. Rec. - Generator	Mailman
X		Bad Code Med Admin	x	DICTATION-Power Scribe		GENDEX	MCCR National Database
		Barcode Medication Administration Contingency Plan (BCU)	x	Dietetics	x	Generic Code Sheet	Meadows (MDWS)
X		BCMA Contingency Workstations	x	Discharge Summary		Genesys	Medicine
		BDN 301	x	DRG Grouper		Get Well Networks	Mental Health
X		Beneficiary Travel	x	DRM Plus		GMED	MHTP
X		Big Fix	x	Drug Accountability	x	GRECC	MICOM
X		CA Verified Components - DSSI	x	DSIT		Health Data and Informatics	Microsoft Exchange E-mail System
X		Capacity Management - RUM	x	DSS Extracts	x	Health Level Seven	Military/Vet Eye Injury Registry
		Capacity Management Tools	x	DSS Quadramed	x	Health Summary	Minimal Patient Dataset
X		CAPRI	x	EDS Whiteboard (AVIED)	x	Health Summary Contingency	Missing Patient Reg (Original) A4EL
		Cardiff Teleform	x	Education Tracking	x	HINQ	Mumps AudioFAX
		Cardiology Systems (stand alone servers from the network)	x	EEO Complaint Tracking	x	Hospital Based Home Care	MyHealthEVet
X		Care Management	x	EKG System	x	ICB	
X		CareTracker		Electronic Card System (ECD)	x	ICR - Immunology Case Registry	
X		CHECKPOINT	x	Electronic Payroll Deduction (EPD)	x	IFCAP	
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: 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
x	National Drug File	x	Pharmacy National Database	Scheduling		VDEF
	National Laboratory Test	x	Pharmacy Prescription Practice	Security Suite Utility Pack	x	Vendor - Document Storage Sys
	NDBI		PICIS OR	Sentillion		Veterans Canteen Web
x	Network Health Exchange	x	Police & Security	Shift Change Handoff Tool	x	Veterans Information Solution
x	NOAHLINK	x	Problem List	ShoreTel		VHAHUNAPP1
	NOIS	x	Progress Notes	Social Work		VHAHUNFP1
	Nursing Service	x	Prosthetics	Stellant		VHS & RA Tracking System
x	Occurrence Screen		Purchase Order Management System	Stentor		Visit Tracking
x	Omnicell	x	Pyxis	Surgery		VISTA RAD
x	Oncology		Q-Matic	Survey Generator	x	VISTA RO
	Onvicond (VLOG)		QMSI Prescription Processing	Telecare Record Manager	x	VistALink
x	Optifill		Quality Assurance Integration	Temp Trak		VistALink Security
x	Order Entry/ Results Reporting		Quality Improvement Checklist	Text Integration Utilities	x	Visual Impairment Service Team ANRV
x	Outpatient Pharmacy	x	QUASER	Tickler Database		Vitria BusinessWare
	P2000 ROBOT	x	Radiology/ Nuclear Medicine	Toolkit		VIXS
x	PACS database		RAFT	TopCon		Voluntary Timekeeping
x	Patch Module	x	RALS	TraceMaster		Voluntary Timekeeping National
x	Patient Data Exchange	x	Record Tracking	Tracking Continuing Education	x	WEB HINQ
	Patient Feedback	x	Registration	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	Utility Management Rollup		Workload and Overtime
	Personal Computer Generated Letters	x	RPC Broker	Utilization Review		
x	Pharmacy Benefits Mangement		Run Time Library	VA Conference Room Registration		
			SAGG	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:	Ft. Meade, SD and Hot Springs, SD making up Black Hills Health Care System (BHHCS)		
Title:	Name:	Phone:	Email:
Privacy Officer:	DanGadomski	605-347-2511x97623	daniel.gadomski@va.gov
Digital Signature Block			
Information Security Officer:	Katherine Vollmer	605-745-2000x92258	katherine.vollmer@va.gov
Digital Signature Block			
System Owner/Delegate:	Stan Bush for BK Hack	612-467-1200	stan.bush@va.gov
Digital Signature Block			
Chief Information Officer:	John Reiffenberger	605-347-7232	john.reiffenberger@va.gov
Digital Signature Block			
Region 2 SMD Reviewer 2/16/2012	Sandra Hedtke	701-237-2566	sandra.hedtke@va.gov
 Sandra Hedtke R2 SMT Reviewer			
Date of Report:	01/2012		
OMB Unique Project Identifier	029-00-02-00-01-1120-00		
Project Name	REGION 2 > VHA > VISN 23 > Black Hills HCS > LAN		
The Signature Process: <ul style="list-style-type: none"> • Complete the PIA form. • Name the PIA Excel FORM ["FY12-Region # - Facility Name - Facility # -Date(mmddyyyy).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(mmddyyyy).xls"] <ul style="list-style-type: none"> • Obtain digital signatures on the "Final Signatures tab" • Submit signed PIA PDF form to the SMART Database. 			

|

|