

Welcome to the PIA for FY 2011!

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.

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.

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.

Directions:

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.

PIA Website: http://vawww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

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. The 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. The 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)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

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 Enable Macros at the prompt.

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

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.

Privacy Impact Assessment Uploaded into SMART

Privacy Impact Assessments should be uploaded into C&A section of SMART.

All PIA Validation Letters should be emailed to christina.pettit@va.gov to received full credit for submission.

(FY 2011) PIA: System Identification

Program or System Name: REGION 2 > VHA > VISN 23 > Sioux Falls VAMC > LAN
 OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-02-00-01-1120-00

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. It uses a standard Server/Client based architecture that communicates using TCP/IP protocol over a star physical

Description of System/ Application/ Program: topology.

Facility Name: Sioux Falls VA Medical Center

Title:	Name:	Phone:	Email:
Privacy Officer:	Karen Mathieu	605.336.3230	karen.mathieu@va.gov
Information Security Officer:	Mary Reifers	605.336.3230	mary.reifers@va.gov
System Owner/ Chief Information Officer:	Stan Bush	612.467.1200	stan.bush@va.gov
Information Owner:	Eric Heiser	605.336.3230	eric.heiser@va.gov
Other Titles:			
Person Completing Document:	Mary Reifers	605.336.3230	mary.reifers@va.gov

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY) 02/2008

Date Approval To Operate Expires: 08/2011

24VA19 Title 38, US Code, Sections 501(b) and 304 also 79VA19 Veterans Health Information Systems and Technology Architecture (VistA), Title 38 US Code section 7301(a).

What specific legal authorities authorize this program or system:

What is the expected number of individuals that will have their PII stored in this system:

1,000,000 – 9,999,999 (our justification is that they are at least 26.8 million veterans records to date)

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.

30 years

Is there an authorized change control process which documents any changes to existing applications or systems?

Yes

If No, please explain:

2. System Identification

Has a PIA been completed within the last three years?

Yes

Date of Report (MM/YYYY):

02/2011

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

- Have any changes been made to the system since the last PIA?
- Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- Does this system/application/program collect, store or disseminate PII/PHI data?
- Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please complete TAB 2 & TAB 12. (See Comment for Definition of PII)

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.

Yes

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

1. All System of Record Identifier(s) (number):

24VA19

24VA19 Title 38, US Code, Sections 501(b) and 304 also 79VA19 Veterans Health Information Systems and Technology Architecture (VistA), Title 38 US Code section 7301(a).

2. Name of the System of Records:

3. Location where the specific applicable System of Records Notice may be accessed (include the URL):

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

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?

Yes

Does the System of Records Notice require modification or updating?

No

(Please Select Yes/No)

Is PII collected by paper methods?

Yes

Is PII collected by verbal methods?

Yes

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

Yes

Proximity and Timing: Is the privacy notice provided at the time of data collection?

Yes

Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

Yes

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

Yes

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

Yes

(FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	ALL	Healthcare, Benefits, Research	All
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Benefits	All
Service Information	ALL	Healthcare, Benefits, Research	All
Medical Information	ALL	Healthcare, Benefits, Research	All
Criminal Record Information	ALL	Benefits	Written
Guardian Information	ALL	Healthcare, Benefits	Written
Education Information	Verbal	Benefits, Research	Written
Benefit Information	ALL	Benefits	All
Other (Explain)			

Data Type	Is Data Type Stored on your system?	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)	Yes	VA Files / Databases (Identify file)	Mandatory
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Mandatory

Service Information	Yes	VA Files / Databases (Identify file)	Mandatory
[Redacted]			
Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory
[Redacted]			
Criminal Record Information	Yes	Other Federal Agency (Identify)	Mandatory
[Redacted]			
Guardian Information	Yes	VA Files / Databases (Identify file)	Mandatory
[Redacted]			
Education Information	Yes	VA Files / Databases (Identify file)	Voluntary
[Redacted]			
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory
[Redacted]			
Other (Explain)			
Other (Explain)			
Other (Explain)			
[Redacted]			

How is a privacy notice provided?

Verbal & Written

Additional Comments

On the Notice of Privacy Practices Form

On the Notice of Privacy Practices Form

On the Notice of Privacy Practices Form



On the Notice of Privacy Practices Form



On the Notice of Privacy Practices Form



On the Notice of Privacy Practices Form



Verbally



On the Notice of Privacy Practices Form



(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization Other Veteran Organization	VBA	Yes	Benefits information & health information for . . .	Both PII & PHI	They access through CAPRI
Other Federal Government Agency	Social Security Admin, IRS, Dept of Treasury, Austin Automation Center, Office of Personnel Management	Yes	Income verification matching with IRS, date of death information with SSA, workload information with Austin Automation Center	PII	All automated
State Government Agency	CDC & the State Dept of Health	No	Public Health Activities/controlling & preventing disease, injury, or disability	Both PII & PHI	Stading Request letter with the State
Local Government Agency					
Research Entity					
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system?	Yes
Please enter the name of the system:	PDX (patient data exchange) will gather information from other VHA sites
Per responses in Tab 4, does the system gather information from an individual?	Yes
If information is gathered from an individual, is the information provided:	<input checked="" type="checkbox"/> Through a Written Request <input checked="" type="checkbox"/> Submitted in Person <input checked="" type="checkbox"/> Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	Yes

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?

Yes

Drug/Alcohol Counseling Mental Health HIV

if yes, please check all that apply:

Research Sickle Cell Other (Please Explain)

Describe process for authorizing access to this data.

Answer: We do Research at our facility, so if the IRB approves a project & the correct waivers or consents are signed & approved then the Researcher may obtain access to the needed data

(FY 2011) PIA: Program Level Questions

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?

No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: Only those questions related to patient care, eligibility, or employment will be asked

How is data checked for completeness?

Answer: Forms are used to ensure no empty fields

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer: Clinical data is not removed. Administrative data is updated with each application for care. Data required to administer health care benefits is validated by personal contact or via use of a VA form. For example, updating of other health insurance information is obtained via VA Form 10-7959c. Computer matching is also utilized via system audits, such as with SSA for SSN and income verification. Patient data is reviewed and updated at each patient episode of care.

How is new data verified for relevance, authenticity and accuracy?

Answer: New data is compared with printed form or via patient verification. Data is matched against supporting documentation submitted by the veteran or beneficiary. Administrative processes are in place to update Human Resources information.

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: From 1 day to 75 years.

Explain why the information is needed for the indicated retention period?

Answer: Record retention is very important to patient care and research

What are the procedures for eliminating data at the end of the retention period?

Answer: Paper is shredded, electronic is degaussed

Where are these procedures documented?

Answer: VA Handbook 6500

How are data retention procedures enforced?

Answer: Nothing is disposed of unless the retention schedule is checked

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

Yes

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2011) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?

No

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 2011) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured. Yes

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.. Yes

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

If 'No' to any of the 3 questions above, please describe why:

Answer:

Is adequate physical security in place to protect against unauthorized access? Yes

If 'No' please describe why:

Answer:

Explain how the project meets IT security requirements and procedures required by federal law.

Answer: At the Department level the CIO's Office of Cyber & Security (OCS) is responsible for the establishment of directives, policies, & procedures which are consistent with the provisions of Federal Information Security Management Act (FISMA) as well as guidance issued by the Office of Management & Budget (OMB), the National Institute of Standards & Technology (NIST), & other requirements that VA is and has been subject to. In addition, OCIS administers and manages Department-wide security solutions, such as anti-virus protection, authentication, vulnerability scanning & penetration testing, & intrusion detection systems, and incident response (800-61). At the project level -The Project Manager ensures that CIO-provided security directives are integrated into the project's security plan & implemented by VA & contractor staff throughout the project. Funding needs are dependent on IT security requirements identified in the system development life cycle (800-64) (i.e. risk assessments (800-30), certification and accreditation (800-37 and 800-53)), as well as identified security weaknesses that must be corrected.

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

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> Air Conditioning Failure | <input checked="" type="checkbox"/> Data Disclosure | <input checked="" type="checkbox"/> Hardware Failure |
| <input type="checkbox"/> Chemical/Biological Contamination | <input checked="" type="checkbox"/> Data Integrity Loss | <input checked="" type="checkbox"/> Identity Theft |
| <input type="checkbox"/> Blackmail | <input checked="" type="checkbox"/> Denial of Service Attacks | <input checked="" type="checkbox"/> Malicious Code |
| <input checked="" type="checkbox"/> Bomb Threats | <input type="checkbox"/> Earthquakes | <input checked="" type="checkbox"/> Power Loss |

- Bomb Threats
- Burglary/Break In/Robbery
- Cold/Frost/Snow
- Communications Loss
- Computer Intrusion
- Computer Misuse
- Data Destruction

- Denial of Service Attacks
- Earthquakes
- Eavesdropping/Interception
- Errors (Configuration and Data Entry)
- Fire (False Alarm, Major, and Minor)
- Flooding/Water Damage
- Fraud/Embezzlement

- Power Loss
- Sabotage/Terrorism
- Storms/Hurricanes
- Substance Abuse
- Theft of Assets
- Theft of Data
- Vandalism/Rioting

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. (Check all that apply)

- Access Control
- Contingency Planning
- Personnel Security
- Audit and Accountability
- Identification and Authentication
- Physical and Environmental Protection
- Awareness and Training
- Incident Response
- Risk Management
- Certification and Accreditation Security Assessments
- Media Protection

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system

Answer: Privacy Notice and Security Controls, C&A

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)

- The potential impact is **low** if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.
- 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.
- The potential impact is **moderate** if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals.

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)

- The potential impact is **low** if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.
-
-

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)

-
-
-



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.

Please add additional controls:

(FY 2011) 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 2011) 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	BCMA Contingency Machines	Automated Medical Information Exchange II (AIME II)
Appraisal System	Benefits Delivery Network (BDN)	Automated Medical Information System (AMIS)290
ASSISTS	Centralized Property Tracking System	Automated Standardized Performace Elements Nationwide (ASPEN)
Awards	Common Security User Manager (CSUM)	Centralized Accounts Receivable System (CARS)
Awards	Compensation and Pension (C&P)	Committee on Waivers and Compromises (COWC)
Baker System	Control of Veterans Records (COVERS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)	Control of Veterans Records (COVERS)	Compensation & Pension Training Website
BDN Payment History	Control of Veterans Records (COVERS)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
BIRLS	Courseware Delivery System (CDS)	Distribution of Operational Resources (DOOR)
C&P Payment System	Dental Records Manager	Educational Assistance for Members of the Selected Reserve Program CH 1606
C&P Training Website	Education Training Website	Electronic Performance Support System (EPSS)
CONDO PUD Builder	Electronic Appraisal System	Enterprise Wireless Messaging System (Blackberry)
Corporate Database	Electronic Card System (ECS)	Financial Management Information System (FMI)
Data Warehouse	Electronic Payroll Deduction (EPD)	Hearing Officer Letters and Reports System (HOLAR)
EndoSoft	Eligibility Verification Report (EVR)	Inquiry Routing Information System (IRIS)
FOCAS	Fiduciary Beneficiary System (FBS)	Modern Awards Process Development (MAP-D)
Inforce	Fiduciary STAR Case Review	Personnel and Accounting Integrated Data and Fee Basis (PAID)
INS - BIRLS	Financial and Accounting System (FAS)	Personal Computer Generated Letters (PCGL)
Insurance Online	Insurance Unclaimed Liabilities	Personnel Information Exchange System (PIES)
Insurance Self Service	Inventory Management System (IMS)	Personnel Information Exchange System (PIES)
LGY Home Loans	LGY Centralized Fax System	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing	Loan Service and Claims	Purchase Order Management System (POMS)
Mobilization	Loan Guaranty Training Website	Reinstatement Entitelment Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Asisstant	Service Member Records Tracking System
Omnicell	National Silent Monitoring (NSM)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Powerscribe Dictation System	Systematic Technical Accuracy Review (STAR)
RAI/MDS	Rating Board Automation 2000 (RBA2000)	Training and Performance Support System (TPSS)
Right Now Web	Rating Board Automation 2000 (RBA2000)	VA Online Certification of Enrollment (VA-ONCE)
SAHSHA	Rating Board Automation 2000 (RBA2000)	VA Reserve Educational Assistance Program
Script Pro	Records Locator System	Veterans Appeals Control and Locator System (VACOLS)
SHARE	Review of Quality (ROQ)	Veterans Assistance Discharge System (VADS)
SHARE	Search Participant Profile (SPP)	Veterans Exam Request Info System (VERIS)
SHARE	Spinal Bifida Program Ch 18	Veterans Service Representative (VSR) Advisor
Sidexis	State Benefits Reference System	Vocational Rehabilitation & Employment (VR&E) CH 31
Synquest	State of Case/Supplemental (SOC/SSOC)	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

VBA Data Warehouse
VBA Training Academy
Veterans Canteen Web
VIC
VR&E Training Website
Web LGY

Telecare Record Manager
VBA Enterprise Messaging System
Veterans On-Line Applications (VONAPP)
Veterans Service Network (VETSNET)
Web Electronic Lender Identification

Web Automated Folder Processing System (WAFPS)
Web Automated Reference Material System (WARMS)
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 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

X ASISTS	X Beneficiary Travel	X Accounts Receivable	X Adverse Reaction Tracking
X Bed Control	X Care Management	ADP Planning (PlanMan)	Authorization/ Subscription
X CAPRI	Care Tracker	X Bar Code Med Admin	Auto Replenishment/ Ward Stock
X CMOP	X Clinical Reminders	Clinical Case Registries	X Automated Info Collection Sys
X Dental	X CPT/ HCPCS Codes	Clinical Procedures	Automated Lab Instruments
X Dietetics	X DRG Grouper	X Consult/ Request Tracking	X Automated Med Info Exchange
X Fee Basis	X DSS Extracts	X Controlled Substances	Capacity Management - RUM
GRECC	Education Tracking	Credentials Tracking	Capacity Management Tools
X HINQ	X Engineering	X Discharge Summary	Clinical Info Resource Network
X IFCAP	X Event Capture	Drug Accountability	Clinical Monitoring System
X Imaging	Extensible Editor	EEO Complaint Tracking	X Enrollment Application System
X Kernal	X Health Summary	X Electronic Signature	Equipment/ Turn-in Request
X Kids	Incident Reporting	Event Driven Reporting	Gen. Med.Rec. - Generator
X Lab Service	X Intake/ Output	External Peer Review	Health Data and Informatics
Letterman	X Integrated Billing	Functional Independence	X ICR - Immunology Case Registry
Library	X Lexicon Utility	Gen. Med. Rec. - I/O	X Income Verification Match
X Mailman	X List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine	Mental Health	X Generic Code Sheet	Interim Mangement Support
MICOM	X MyHealthEVet	X Health Level Seven	X Master Patient Index VistA
NDBI	X National Drug File	X Hospital Based Home Care	Missing Patient Reg (Original) A4EL
NOIS	X Nursing Service	X Inpatient Medications	X Order Entry/ Results Reporting
Oncology	Occurrence Screen	X Integrated Patient Funds	X PCE Patient Care Encounter
PAID	Patch Module	MCCR National Database	Pharmacy Benefits Mangement
X Prosthetics	Patient Feedback	Minimal Patient Dataset	Pharmacy Data Management
X QUASER	X Police & Security	National Laboratory Test	Pharmacy National Database
X RPC Broker	X Problem List	X Network Health Exchange	Pharmacy Prescription Practice
SAGG	X Progress Notes	X Outpatient Pharmacy	Quality Assurance Integration
X Scheduling	X Record Tracking	Patient Data Exchange	Quality Improvement Checklist
Social Work	X Registration	Patient Representative	X Radiology/ Nuclear Medicine
X Surgery	Run Time Library	PCE Patient/ HIS Subset	X Release of Information - DSSI
X Toolkit	Survey Generator	Security Suite Utility Pack	Remote Order/ Entry System
Unwinder	Utilization Review	Shift Change Handoff Tool	Utility Management Rollup
X VA Fileman	Visit Tracking	Spinal Cord Dysfunction	CA Verified Components - DSSI
X VBECS	VistALink Security	X Text Integration Utilities	Vendor - Document Storage Sys
VDEF	X Women's Health	VHS & RA Tracking System	Visual Impairment Service Team ANRV
VistALink		Voluntary Timekeeping	Voluntary Timekeeping National

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 2011) PIA: Minor Applications

Which of these are sub-components of your system?

1184 Web	ENDSOFT	RAFT
	Enterprise Terminology Server &	RALS
A4P	VHA Enterprise Terminology	
	Services	X

Date of Report:

2/25/2011

OMB Unique Project Identifier

029-00-02-00-01-1120-00

Project Name

REGION 2 > VHA > VISN 23 > Sioux

Falls VAMC > LAN

Email:

karen.mathieu@va.gov

mary.reifers@va.gov

stan.bush@va.gov

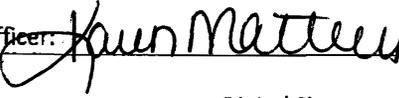
eric.heiser@va.gov

0

(FY 2011) PIA: Final Signatures

Facility Name: REGION 2 > VHA > VISN 23 > Sioux Falls VAMC > LAN

Title: Name: Phone:

Privacy Officer:  Karen Mathieu 605.336.3230
x6680

Digital Signature Block

Information Security Officer:  Mary Reifers 605.336.3230
x6641

Digital Signature Block

System Owner/ Chief Information Officer: BK Hack, Director, Region 2 OI&T
Field Operations Stan Bush,
Network Chief Information Officer
on behalf of BH Hack

 612.467.1200

Digital Signature Block

Information Owner:  Eric Heiser 605.336.3230
x6862

Digital Signature Block

Other Titles: 0 0

Digital Signature Block