

## **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](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](mailto:christina.pettit@va.gov) to received full credit for submission.

## (FY 2011) PIA: System Identification

**Program or System Name:** LAN REGION 1 > VHA > VISN 20 > Spokane VAMC > LAN  
 OMB Unique System / Application / Program Identifier (AKA: UPID #): Exhibit: 300 ID: 029-00-02-00-01-1120-00  
 Description of System/ Application/ Program: The Local Area Network (LAN) is a general support system providing basic network connectivity to enterprise systems and access to desktop applications. The VA Spokane VAMC LAN is one of eight subordinate VA Medical center data networks within Veterans Integrated Service Network 20 (VISN 20) - a regional organization of VA hospitals and remote medical clinics. Within the scope of the VA Spokane VAMC LAN are the main hospital campus and five remote satellite facilities including two CBOC's and one Veteran's Center. **\*\*Please see Additional Comments tab\*\***

Facility Name:	Spokane VAMC		
<b>Title:</b>	<b>Name:</b>	<b>Phone:</b>	<b>Email:</b>
Privacy Officer:	Alanna Dobson	509-434-7525	<a href="mailto:alanna.dobson@va.gov">alanna.dobson@va.gov</a>
Information Security Officer:	Kenneth Klein	509-434-7502	<a href="mailto:kenneth.klein@va.gov">kenneth.klein@va.gov</a>
System Owner/ Delegation of Authority	Robert Fortenberry	509-434-7430	<a href="mailto:robert.fortenberry@va.gov">robert.fortenberry@va.gov</a>
Other Titles:			
Other Titles:			
Person Completing Document:	Alanna Dobson	509-434-7525	<a href="mailto:alanna.dobson@va.gov">alanna.dobson@va.gov</a>
Person Completing Document:	Kenneth Klein	509-434-7502	<a href="mailto:kenneth.klein@va.gov">kenneth.klein@va.gov</a>
Person Completing Document:	Robert Fortenberry	509-434-7430	<a href="mailto:robert.fortenberry@va.gov">robert.fortenberry@va.gov</a>
Person Completing Document:	Aimee Swanson	509-434-7000	<a href="mailto:aimee.swanson@va.gov">aimee.swanson@va.gov</a>
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)			06/2008
Date Approval To Operate Expires:			08/2011

What specific legal authorities authorize this program or system: 24 VA19 Patient Medical Records  
 What is the expected number of individuals that will have their PII stored in this system: Between 50,000-200,000 patients and 3,000 to 8,000 employees.  
 Identify what stage the System / Application / Program is at: Operations/Maintenance  
 The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation. Approx. 20 years  
 Is there an authorized change control process which documents any changes to existing applications or systems? Yes  
 If No, please explain:  
 Has a PIA been completed within the last three years? Yes  
 Date of Report (02/2011) 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? Yes they no longer belong to Spokane but are now under region 1.
- 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? No
- Does this system/application/program collect, store or disseminate the SSN? No

**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):

SOR 79 VA 19, Privacy Act, 5 U.S.C. 552a(e)(4)

2. Name of the System of Records:

(VISTA)-VA Veterans Health Information System and  
Technology Architecture - Patient Medical Records - VA

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

<http://vaww.vhaco.va.gov/privacy/systemofRecords.htm>

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?

No

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?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	ALL	Collection is only for payment of invoices	All	Verbal & Written
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Collection is only for entitlement payments	All	Verbal & Written
Service Information	ALL	Collection is for eligibility	All	Verbal & Written
Medical Information	Paper & Electronic	Collection is for eligibility and payment of invoices	Verbal & Automatic	Verbal & Written
Criminal Record Information		N/A		
Guardian Information		N/A		
Education Information		N/A		
Benefit Information	Electronic/File Transfer	Collection is for eligibility and payment of invoices	Verbal & Written	Verbal & Written
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?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran/Beneficiary/Sponsor	Mandatory	The intended use of this information is to appropriately identify the patient and accurately link patient records under VA systems as appropriate to provide for accurate clinical decision making and continuity of care. <b>Beneficiaries sign 'Release of Information Waivers' which are kept on file. We reject claims that indicate the ROI statement is not onfile. It is on the Application for Benefits.</b>

Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran/Beneficiary/Sponsor	Mandatory	Next of Kin and Emergency Contact information; names, addresses, phone numbers. Used for notification in case of emergency.
Service Information	Yes	Veteran/Sponsor/VA Databases	Mandatory	Military branch, rank, discharge information, and dates of service - as described on the official DD-214. Service Information for both benefits and Eligibility needs
Medical Information	Yes	Veteran/Beneficiary/Sponsor/Provider	Mandatory	Diagnosis, medical history, current problem list, prescriptions, surgeries and family history All medical information is to provide care to veterans. The clinicians have the responsibility to distinguish between relevant and irrelevant information that relates to the care of the veteran.
Criminal Record Information	Yes	Veteran	Mandatory	Name, SSN, DOB, Address, Telephone numbers, Geographic location. Required by Federal statute to identify wanted felons.
Guardian Information	Yes	Veteran/Beneficiary/Sponsor	Mandatory	Yes, where applicable. Guardian information on those veterans where necessary for identification and benefit disbursement, as well as medical decision-making factors.
Education Information	Yes	Veteran/Beneficiary/Sponsor	Mandatory	
Benefit Information	Yes	Veteran/Sponsor/VA Databases	Mandatory	
Other (Explain)				
Other (Explain)				
Other (Explain)				

(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	All VA	Yes	Invoices for payment purposes	Both PII & PHI	24VA19, Privacy and HIPAA rules
Other Veteran Organization		No		N/A	
Other Federal Government Agency		No		N/A	
State Government Agency		No		N/A	
Local Government Agency		No		N/A	
Research Entity		No		N/A	
Other Project / System	Virtual Lifetime Electroinc Record/National Health Information Network - NHIN	No	Pilot site for VLER / Coordination of care with the DoD, VA & INHS thru NHIN electronic information exchange	Both PII & PHI	VLER Implementation Team material
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system? No

Please enter the name of the system:

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:

- Through a Written Request
- Submitted in Person
- 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? No

if yes, please check all that apply:

- Drug/Alcohol Counseling
- Mental Health
- HIV
- Research
- Sickle Cell
- Other (Please Explain)

Describe process for authorizing access to this data.  
 Answer: Requires patient authorization

## (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: Minimum amount necessary. The collected data is entered into the application pertaining to the specified requirement and is not accessible outside the required applications.

How is data checked for completeness?

Answer: Verified by clerk. Applications have predetermined fields for entry and/or are reviewed by department quality assurance resources.

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

Answer: Verified by clerk. Periodical reports are run per application to ensure accuracy and currency, where applicable.

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

Answer: Verified by clerk. Data source providers are responsible for the relevance, authenticity and accuracy within each of the systems they operate.

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

Answer: None

## (FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: Records are retained on tape and electronic media for 6 years and 3 months as required by National Archive Records; 6yrs, 3 months after beneficiary is no longer eligible for services

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

Answer: To verify eligibility and to process or audit claims per VA guidelines; Retention periods are governed by General Accounting Office Regulations which require retention for records created prior to July 2, 1975; 10 years and 3 months after the period of the account; records created on or after July 2, 1975; 6 years and 3 months from the period of the account. Information is needed for general auditing and accounting purposes.

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

Answer: Files are removed under VA Schedule of Records 10-1, section 38. File plans were developed for each Service identifying what records were required to be maintained. Annual records management reviews will be developed and conducted to either destroy or move data to appropriate temporary storage until disposition date is reached.

Where are these procedures documented?

Answer: VA Schedule of Records 10-1, section 38

How are data retention procedures enforced?

Answer: Yearly Record Management Reviews and VA Directive 6300.1. Record Manager performs annual inventory

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

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

Answer: Record Manager Program is currently being implemented and retention schedule has not been created yet. Annual record reviews will be conducted within each service who is responsible for the major system which stores their information.

## (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 <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Is security testing conducted on at <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Are performance evaluations conducted on at <u>least</u> 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: By having the C&A process in place and multiple agency checks to insure all is compliant.

- 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 checked="" type="checkbox"/> Chemical/Biological Contamination | <input type="checkbox"/> Data Integrity Loss                              | <input checked="" type="checkbox"/> Identity Theft     |
| <input checked="" type="checkbox"/> Blackmail                         | <input checked="" type="checkbox"/> Denial of Service Attacks             | <input checked="" type="checkbox"/> Malicious Code     |
| <input checked="" type="checkbox"/> Bomb Threats                      | <input checked="" type="checkbox"/> Earthquakes                           | <input type="checkbox"/> Power Loss                    |
| <input type="checkbox"/> Burglary/Break In/Robbery                    | <input checked="" type="checkbox"/> Eavesdropping/Interception            | <input checked="" type="checkbox"/> Sabotage/Terrorism |
| <input checked="" type="checkbox"/> Cold/Frost/Snow                   | <input checked="" type="checkbox"/> Errors (Configuration and Data Entry) | <input checked="" type="checkbox"/> Storms/Hurricanes  |
| <input checked="" type="checkbox"/> Communications Loss               | <input checked="" type="checkbox"/> Fire (False Alarm, Major, and Minor)  | <input checked="" type="checkbox"/> Substance Abuse    |
| <input checked="" type="checkbox"/> Computer Intrusion                | <input checked="" type="checkbox"/> Flooding/Water Damage                 | <input checked="" type="checkbox"/> Theft of Assets    |
| <input checked="" type="checkbox"/> Computer Misuse                   | <input checked="" type="checkbox"/> Fraud/Embezzlement                    | <input checked="" type="checkbox"/> Theft of Data      |
| <input type="checkbox"/> Data Destruction                             |   | <input checked="" type="checkbox"/> Vandalism/Rioting  |

Answer: (Other Risks)

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"/> Contingency Planning              | <input checked="" type="checkbox"/> Personnel Security                    |
| <input checked="" type="checkbox"/> Audit and Accountability                             | <input checked="" type="checkbox"/> Identification and Authentication | <input checked="" type="checkbox"/> Physical and Environmental Protection |
| <input checked="" type="checkbox"/> Awareness and Training                               | <input checked="" type="checkbox"/> Incident Response                 | <input checked="" type="checkbox"/> Risk Management                       |
| <input checked="" type="checkbox"/> Certification and Accreditation Security Assessments |   |   |
| <input checked="" type="checkbox"/> Configuration Management                             | <input checked="" type="checkbox"/> Media Protection                  |   |

Answer: (Other Controls)

### PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Exactly the same as last time except that it no longer belongs to us and we don't even have a LAN manager! Collection sources and security controls.

<b>Availability Assessment:</b> 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)	<input checked="" type="checkbox"/> The potential impact is <b>high</b> 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 <b>moderate</b> 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 <b>low</b> if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

<b>Integrity Assessment:</b> If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? (Choose One)	<input checked="" type="checkbox"/> The potential impact is <b>high</b> 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 <b>moderate</b> 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 <b>low</b> if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.

<b>Confidentiality Assessment:</b> If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? (Choose One)	<input checked="" type="checkbox"/> The potential impact is <b>high</b> 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 <b>moderate</b> 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 <b>low</b> 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.

Please add additional controls:

The availability, integrity and confidentiality assessment was high for the LAN and Vista however we no longer have these systems. Our only system now is PBX and it is rated as low.

The availability, integrity

PIA: Additional Comments

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.

The Spokane VAMC is one of only four stations nationwide that has no local storage of data. All data, whether generated by office automation applications, e.g., MS Word, or VistA, is stored, via real-time transmission, at the VA OI&T Region 1 Regional Data Center in Sacramento, California. The RDC provides all backup storage of all medical systems as well. The Sacramento RDC is backed up by a real-time "roll-over" RDC in Denver, Colorado. Additioanally, Spokane VAMC empolyees are not able to "write"/save files to their local harddrives, only to their network shares/folders (located in Sacramento.)

(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 Entitlement 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	Telecare Record Manager	Web Automated Folder Processing System (WAFPS)
VBA Training Academy	VBA Enterprise Messaging System	Web Automated Reference Material System (WARMS)
Veterans Canteen Web	Veterans On-Line Applications (VONAPP)	Web Automated Verification of Enrollment
VIC	Veterans Service Network (VETSNET)	Web-Enabled Approval Management System (WEAMS)
VR&E Training Website	Web Electronic Lender Identification	Web Service Medical Records (WebSMR)
Web LGY		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	x ADP Planning (PlanMan)	x Authorization/ Subscription
x CAPRI	x Care Tracker	x Bad Code Med Admin	x Auto Replenishment/ Ward Stock
x CMOP	x Clinical Reminders	x Clinical Case Registries	x Automated Info Collection Sys
x Dental	x CPT/ HCPCS Codes	x Clinical Procedures	x 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	x Capacity Management - RUM
x GRECC	x Education Tracking	x Credentials Tracking	x Capacity Management Tools
x HINQ	x Engineering	x Discharge Summary	x Clinical Info Resource Network
x IFCAP	x Event Capture	x Drug Accountability	x Clinical Monitoring System
x Imaging	x Extensible Editor	x EEO Complaint Tracking	x Enrollment Application System
x Kernal	x Health Summary	x Electronic Signature	x Equipment/ Turn-in Request
x Kids	x Incident Reporting	x Event Driven Reporting	x Gen. Med.Rec. - Generator
x Lab Service	x Intake/ Output	x External Peer Review	x Health Data and Informatics
x Letterman	x Integrated Billing	x Functional Independence	x ICR - Immunology Case Registry
x Library	x Lexicon Utility	x Gen. Med. Rec. - I/O	x Income Verification Match
x Mailman	x List Manager	x Gen. Med. Rec. - Vitals	x Incomplete Records Tracking
x Medicine	x Mental Health	x Generic Code Sheet	Interim Mangement Support
x MICOM	x MyHealthEVet	x Health Level Seven	x Master Patient Index VistA
x NDBI	x National Drug File	x Hospital Based Home Care	x Missing Patient Reg (Original) A4EL
x NOIS	x Nursing Service	x Inpatient Medications	x Order Entry/ Results Reporting
x Oncology	x Occurrence Screen	x Integrated Patient Funds	x PCE Patient Care Encounter
x PAID	x Patch Module	x MCCR National Database	x Pharmacy Benefits Mangement
x Prosthetics	x Patient Feedback	x Minimal Patient Dataset	x Pharmacy Data Management
x QUASER	x Police & Security	x National Laboratory Test	x Pharmacy National Database
x RPC Broker	x Problem List	x Network Health Exchange	x Pharmacy Prescription Practice
x SAGG	x Progress Notes	x Outpatient Pharmacy	x Quality Assurance Integration
x Scheduling	x Record Tracking	x Patient Data Exchange	x Quality Improvement Checklist
x Social Work	x Registration	x Patient Representative	x Radiology/ Nuclear Medicine
x Surgery	x Run Time Library	x PCE Patient/ HIS Subset	x Release of Information - DSSI
x Toolkit	x Survey Generator	x Security Suite Utility Pack	x Remote Order/ Entry System
Unwinder	x Utilization Review	x Shift Change Handoff Tool	x Utility Management Rollup
x VA Fileman	x Visit Tracking	x Spinal Cord Dysfunction	x CA Verified Components - DSSI
x VBECS	x VistALink Security	x Text Integration Utilities	x Vendor - Document Storage Sys
x VDEF	x Women's Health	x VHS & RA Tracking System	x Visual Impairment Service Team ANRV
x VistALink		x Voluntary Timekeeping	x 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	Vista Visual Aid
Description	appointment display-only application
Comments	VISN 20 approved application
Is PII collected by this minor application?	NO
Does this minor application store PII?	NO
If yes, where?	N/A
Who has access to this data?	Point of care staff; IT staff; staff with Vista access and menu assignment

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
A4P	x	Enterprise Terminology Server & VHA Enterprise Terminology Services	x	RALS
Administrative Data Repository (ADR)	x	ePROMISE	x	Remedy Application
ADT	x	EYECAP		SAN
Agent Cashier	x	Financial and Accounting System (FAS)		Scanning Exam and Evaluation System
Air Fortress	x	Financial Management System	x	Sentillion
Auto Instrument		Genesys		Stellant
Automated Access Request	x	Health Summary Contingency		Stentor
BDN 301		ICB		Tracking Continuing Education
Bed Board Management System	x	KOWA	x	Traumatic Brain Injury
Cardiff Teleform		Lynx Duress Alarm	x	VA Conference Room Registration
Cardiology Systems (stand alone servers from the network)		MHTP		VAMedSafe
CHECKPOINT	x	Microsoft Active Directory	x	VBA Data Warehouse
Clinical Data Repository/Health Data Repository	x	Microsoft Exchange E-mail System		
Combat Veteran Outreach Committee on Waiver and Compromises	x	Military/Vet Eye Injury Registry		VHAHUNAPP1 VHAHUNFPC1
CP&E	x	Mumps AudioFAX	x	VISTA RAD
Crystal Reports Enterprise Data Innovations	x	NOAHLINK		Whiteboard
DELIVEREX		Omnicell		
DICTION-Power Scribe	x	Onvicord (VLOG)		
DRM Plus	x	Optifill		
		P2000 ROBOT		
		PACS database	x	

x	DSIT		Personal Computer Generated Letters
x	DSS Quadramed		PICIS OR
	EDS Whiteboard (AVJED)	x	PIV Systems
	EKG System		Q-Matic
x	Embedded Fragment Registry		QMSI Prescription Processing

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: Final Signatures

Facility Name: REGION 1> VHA > VISN 20 > Spokane VAMC > LAN

Title:	Name:	Phone:	Email:
--------	-------	--------	--------

Privacy Officer:	Alanna Dobson	509-434-7525	alanna.dobson@va.gov
------------------	---------------	--------------	----------------------

Digital Signature Block
-------------------------

Information Security Officer:	Kenneth Klein	509-434-7502	kenneth.klein@va.gov
-------------------------------	---------------	--------------	----------------------

Digital Signature Block
-------------------------

System Owner/ Delegation of Authority	Robert Fortenberry	509-434-7430	robert.fortenberry@va.gov
---------------------------------------	--------------------	--------------	---------------------------

Digital Signature Block
-------------------------

Other Titles:	0	0	0
---------------	---	---	---

Digital Signature Block
-------------------------

Other Titles:	0	0	0
---------------	---	---	---

Digital Signature Block
-------------------------

Date of Report: 2/28/11

OMB Unique Project Identifier Exhibit: 300 ID: 029-00-02-00-01-1120-00

Project Name REGION 1> VHA > VISN 20 > Spokane VAMC > LAN