

(FY 2011) PIA: System Identification

Program or System Name: REGION 2 > VHA > VISN 16> Shreveport VAMC > LAN
 OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-02-00-01-1120-00

Description of System/ Application/ Program: The LAN system is comprised of workstation, servers, printers and other equipment which include devices such as routers, hubs, switches, and firewalls that support communications to extended LAN locations such as CBOC's. The LAN system also includes subsystem components such as tape drives, disk drives, UPS', NAS' and SAN's.

Facility Name: Shreveport VAMC

Title:	Name:	Phone:	Email:
Privacy Officer:	Judy Boogaerts	318-990-6711	judy.boogaerts@va.gov
Information Security Officer:	Michael N. Brown	318-990-5055	michael.brown5@va.gov
System Owner/ Chief Information Officer:	Janey Taylor	318-990-5555	janey.taylor2@va.gov
Information Owner:	R. Dale Nelson	479-444-5011	dale.nelson1@va.gov
Other Titles: Network Manager	Brian Jackson	318-990-5555	brian.jackson@va.gov
Person Completing Document:	Shacoria Williams	318-990-4839	shacoria.williams@va.gov

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY) 07/2009

Date Approval To Operate Expires: 06/2011

What specific legal authorities authorize this program or system: Title 38, United States Code, Section 7301 (a)

What is the expected number of individuals that will have their PII stored in this system: 1,000,000 - 9,999,999

Identify what stage the System / Application / Program is at: Operations/Maintenance

The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation. 16 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 (MM/YYYY): 01/2011

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 7 & 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, 79VA19

2. Name of the System of Records:

Patient Medical Records; VistA 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?

No

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

No

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

No

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

No

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

No

(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?
Service Information	VA File Database	Benefits	Verbally	Verbally
Criminal Record Information	VA File Database	Eligibility for employment	Verbally	Verbally
Education Information	VA File Database	Eligibility for employment	Verbally	Verbally
Benefit Information	VA File Database	Eligibility for employment	Verbally	Verbally
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
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Criminal Record Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Education Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Benefit Information	Yes	VA Files / Databases (Identify file)	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	Other VA hospitals, VBA, National Cemetary, VA Police	Yes	Employee Information	PII	VHA 1605.1 and 1605.2
Other Veteran Organization					
Other Federal Government Agency	OPM	No		PII	Employment Benefits
State Government Agency	Louisiana War Veterans Homes;	Yes	Access Only	PII	VA Directive
Local Government Agency	Law enforcement	No			VA Directive
Research Entity	Louisiana State University Health Sciences Center	Yes	Access Only	N/A	VA Directive
Other Project / System	Bar Code Medication Administration (BCMA)	Yes	Access Only	N/A	VA Directive
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:	<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?	No
---	----

if yes, please check all that apply: Research Sickle Cell Mental Health HIV

Describe process for authorizing access to this data.

Answer: Identities are checked and verified along with whether the person needs the information in the performance of their duties.

(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: Menu hierarchy

How is data checked for completeness?

Answer: Reviewed by OI&T, ISO, and PO. There are also system triggers for missing or incomplete data.

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

Answer: PIA reviewed annually or at time of any change to the system.

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

Answer: Performance Measure Monitors; Chart Review, EPRP Review

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: Data is destroyed 75 years after the last episode of use.

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

Answer: For health care and determination of veteran benefits

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

Answer: Federal Records Centers destroys based on date of retirement

Where are these procedures documented?

Answer: VA Handbook 6300; RCS 10-1

How are data retention procedures enforced?

Answer: Program officials, records managers, field record officers, and all VA employees are responsible for following all directives and guidance for

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: We follow all IT security requirements and procedures as set by federal law.

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 checked="" 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 type="checkbox"/> Earthquakes | <input checked="" type="checkbox"/> Power Loss |
| <input checked="" 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 checked="" 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)

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

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.

Answer: Increase vigilance in protecting our systems and provide more employee training.

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

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	X	BCMA Contingency Machines		Automated Medical Information Exchange II (AIME II)
Appraisal System		Benefits Delivery Network (BDN)		Automated Medical Information System (AMIS)290
X 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)	X	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	X	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
X MUSE	X	Mental Health Asisstant		Service Member Records Tracking System
X Omnicell		National Silent Monitoring (NSM)		Survivors and Dependents Education Assistance CH 35
X 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
X 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
X 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	X 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
X 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
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	x Interim Mangement Support
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
x 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
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
A4P	Enterprise Terminology Server & VHA Enterprise Terminology Services	RALS

(FY 2011) PIA: Final Signatures

Facility Name: REGION 2 > VHA > VISN 16> Shreveport VAMC > LAN

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

Privacy Officer:	Judy Boogaerts	318-990-6711	judy.boogaerts@va.gov
------------------	----------------	--------------	-----------------------

2/3/2011

X 

Judy Boogaerts
Privacy Officer

Information Security Officer:	Michael N. Brown	318-990-5055	michael.brown5@va.gov
-------------------------------	------------------	--------------	-----------------------

2/22/2011

X 

Michael N. Brown
Facility ISO

System Owner/ Chief Information Officer:	Janey Taylor	318-990-5555	janey.taylor2@va.gov
--	--------------	--------------	----------------------

2/23/2011

X 

Janey Taylor
Facility CIO

Information Owner:	R. Dale Nelson	479-444-5011	dale.nelson1@va.gov
--------------------	----------------	--------------	---------------------

2/25/2011

X 

R. Dale Nelson
N16 CIO

Other Titles: Network Manager

Brian Jackson

318-990-5555

brian.jackson@va.gov

2/22/2011

X Brian Jackson

Brian Jackson
Network Manager

Date of Report:

1/25/11

OMB Unique Project Identifier

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

Project Name

REGION 2 > VHA > VISN 16>

Shreveport VAMC > LAN