

## (FY 2010) PIA: System Identification

---

Program or System Name: REGION 2 > VHA > VISN 15 >  
Columbia VAMC > LAN

OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-02-00-01-1120-00

The Columbia, MO VAMC LAN is 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 VistA, medical imaging, supply management, decision support, medical research, human resources, business operations and

Description of System / Application / Program: education.

---

Facility Name: Harry S Truman Memorial Veterans Hospital

Title:	Name:	Phone:	Email:
Privacy Officer:	Ann Richmond	573-814-6589	<a href="mailto:ann.richmond@va.gov">ann.richmond@va.gov</a>

Information Security Officer:	Kevin Sample	573-814-6250	<a href="mailto:kevin.sample@va.gov">kevin.sample@va.gov</a>
Chief Information Officer:	Donna Krause	573-814-6501	<a href="mailto:donna.krause@va.gov">donna.krause@va.gov</a>
Person Completing Document:	All designees listed above		
Other Titles:			

Other Titles:

Other Titles:

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

01/2008

Date Approval To Operate Expires:

08/2011

---

90VA194  
34VA12  
89VA19  
113VA112  
77VA10Q  
What specific legal authorities authorize this program or system: 121VA19  
24VA19  
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.  
10/1986  
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?

Date of Report (MM/YYYY): 03/2010

**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 skip to TAB 12. ( See Comment for Definition of PII)**

(FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?

Yes

if the answer above is no, please skip to row 16.

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

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

113VA112 Telephone Care and Service Records-  
VA 77VA19 Health Care  
Provider Credentialing and Priviledging Records -  
VA 34VA12 Veteran, Patient,  
Employee and Volunteer Research and  
Development Project Records-VA  
90VA194 Call Detail Records - VA  
121VA19 – National Patient Databases  
24VA19 Patient Medical Records - VA  
89VA19 - Health Eligibility Records  
[http://www.va.gov/privacy/Update  
SOR/SOR24VA19.pdf](http://www.va.gov/privacy/UpdateSOR/SOR24VA19.pdf)  
[http://www.va.gov/privacy/Update  
SOR/SOR90VA194.pdf](http://www.va.gov/privacy/UpdateSOR/SOR90VA194.pdf)

2. Name of the System of Records:

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

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?

No

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 2010) 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)	Verbal	Privacy Notice	Verbally	Verbally
Family Relation (spouse, children, parents, grandparents, etc)	VA File Database	Privacy Notice	Written	Written
Service Information	Electronic/File Transfer	Privacy Notice	Verbally	Written
Medical Information	Paper	Privacy Notice	Verbally	Written
Criminal Record Information	VA File Database	Privacy Notice	Written	Written
Guardian Information	Paper	Privacy Notice	Written	Written
Education Information	Paper	Privacy Notice	Written	Written
Benefit Information	Paper	Privacy Notice	Written	Written
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source requested, identify the specific file, entity and/or name of agency	(If Is data collection Mandatory or Voluntary?	Additional Comments
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	Veteran	Voluntary	
Service Information	Yes	Other Federal Agency (Identify)	Mandatory	
Medical Information	Yes	Veteran	Voluntary	
Criminal Record Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Guardian Information	Yes	Veteran	Voluntary	
Education Information	Yes	Veteran	Voluntary	
Benefit Information	Yes	Veteran	Mandatory	
Other (Explain)				
Other (Explain)				
Other (Explain)				

(FY 2010) 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	VA Regional Counsel (VBA); Veterans Benefits Administration (VBA)	Yes	payment, treatment and healthcare operations	Both PII & PHI	Ref. 45 CFR 164.512; 5 USC 552a[b]; 38 USC 7332[b]; 38 USC 5701[b]
Other Veteran Organization				Both PII & PHI	Ref. 45 CFR 164.512; 5 USC 552a[b]; 38 USC 7332[b]; 38 USC 5701[b]
Other Federal Government Agency	Paralyzed Veterans of America, Veterans of Foreign Wars	Yes	payment, treatment and healthcare operations	Both PII & PHI	Ref. 45 CFR 164.512; 5 USC 552a[b]; 38 USC 7332[b]; 38 USC 5701[b]
State Government Agency	St. James Vet Home, Mexico Vet Home	Yes	payment, treatment and healthcare operations	Both PII & PHI	CPRS Read-Only Access VHA Directive, VA Form 10-5345
Local Government Agency	None				
Research Entity	University of Missouri	Yes	Patient Health Records for Research purposes	Both PII & PHI	VHA Handbook 1200.12
Other Project / System	QuadraMed	Yes	Data is not shared. Vendor	Both PII & PHI	National BAA
Other Project / System	CMOP, Pharmacy, Bio-Medical Vendors	Yes	payment, treatment and healthcare operations	Both PII & PHI	Ref. 45 CFR 164.512; 5 USC 552a[b]; 38 USC 7332[b]; 38 USC 5701[b]
Other Project / System	None				

(FY 2010) PIA: Access to Records

Does the system gather information from another system?

Yes

Please enter the name of the system:

Health Eligibility Center (HEC), U.S. Postal Service, Internal Revenue Service

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 2010) PIA: Secondary Use

Will PII data be included with any secondary use request?  
Yes

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.

Local policy reflecting VA Handbook and Directives 6500, VHA Handbooks 1605.1 and 1605.3 and HSTVAH Privacy Policy regarding Minimum Necessary per VHA Handbook 1605.2

Answer:

### (FY 2010) 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: Functional category and Minimum Necessary standards per Directive 1605.

How is data checked for completeness?

Answer: Each Service Line conducts monitors and audits per regulatory requirements (i.e. IG, JC, etc.).

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

Answer: Patient information is updated and/or verified at pt. visits, (i.e. Means Test,

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

Answer: Internal Medical Center Policies & Controls

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

Answer:

### (FY 2010) PIA: Retention & Disposal

What is the data retention period?

Answer: Per RCS 10-1 and GSA

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

Answer: To comply with Federal Law and facilitate the mission of the VA

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

Answer: HSTVAH follows VA and VHA Records Management Handbooks and Directives including RCS 10-1 and GRS. Local Policy and designation of responsibilities in place

Where are these procedures documented?

Answer: VA Publications and VAMC Columbia Records Management Policy and Procedures

How are data retention procedures enforced?

Answer: VA Publications

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 2010) 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: N/A

---

(FY 2010) 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: Facility follows VA 6500 based on NIST 800-53 guidance

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

Answer: (Other Risks)

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

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

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: No change to data collection made, implementation of records inventory and file plan to be initiated

**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 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.

**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 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.

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 2010) PIA: Additional Comments**

---

Add any additional comments on this tab for any question in the form you want to comment on.  
Please indicate the question you are responding to and then add your comments.

---

(FY 2010) PIA: VBA Minor Applications

Explain what minor application that are associated with your installation? (Check all that apply)

	N/A	
Records Locator System	Education Training Website	Appraisal System
Veterans Assistance Discharge System (VADS)	VR&E Training Website	Web Electronic Lender Identification
LGY Processing	VA Reserve Educational Assistance Program	CONDO PUD Builder
Loan Service and Claims	Web Automated Verification of Enrollment	Centralized Property Tracking System
LGY Home Loans	Right Now Web	Electronic Appraisal System
Search Participant Profile (SPP)	VA Online Certification of Enrollment (VA-ONCE)	Web LGY
Control of Veterans Records (COVERS)	Automated Folder Processing System (AFPS)	Access Manager
SHARE	Personal Computer Generated Letters (PCGL)	SAHSHA
Modern Awards Process Development (MAP-D)	Personnel Information Exchange System (PIES)	VBA Data Warehouse
Rating Board Automation 2000 (RBA2000)	Rating Board Automation 2000 (RBA2000)	Distribution of Operational Resources (DOOR)
State of Case/Supplemental (SOC/SSOC)	SHARE	Enterprise Wireless Messaging System (Blackberry)
Awards	State Benefits Reference System	VBA Enterprise Messaging System
Financial and Accounting System (FAS)	Training and Performance Support System (TPSS)	LGY Centralized Fax System
Eligibility Verification Report (EVR)	Veterans Appeals Control and Locator System (VACOLS)	Review of Quality (ROQ)
Automated Medical Information System (AMIS)290	Veterans On-Line Applications (VONAPP)	Automated Sales Reporting (ASR)
Web Automated Reference Material System (WARMS)	Automated Medical Information Exchange II (AIME II)	Electronic Card System (ECS)
Automated Standardized Performance Elements Nationwide (ASPEN)	Committee on Waivers and Compromises (COWC)	Electronic Payroll Deduction (EPD)
Inquiry Routing Information System (IRIS)	Common Security User Manager (CSUM)	Financial Management Information System (FMI)
National Silent Monitoring (NSM)	Compensation and Pension (C&P)	Purchase Order Management System (POMS)
Web Service Medical Records (WebSMR)	Record Interchange (CAPRI)	Veterans Canteen Web
Systematic Technical Accuracy Review (STAR)	Control of Veterans Records (COVERS)	Inventory Management System (IMS)
Fiduciary STAR Case Review	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)	
Veterans Exam Request Info System (VERIS)	Fiduciary Beneficiary System (FBS)	Synquest
Web Automated Folder Processing System (WAFPS)	Hearing Officer Letters and Reports System (HOLAR)	RAI/MDS
	Inforce	ASSISTS
Courseware Delivery System (CDS)	Awards	MUSE
Electronic Performance Support System (EPSS)	Actuarial	Bbraun (CP Hemo)
Veterans Service Representative (VSR) Advisor	Insurance Self Service	VIC
Loan Guaranty Training Website	Insurance Unclaimed Liabilities	BCMA Contingency Machines
C&P Training Website	Insurance Online	Script Pro

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
<input type="checkbox"/> Is PII collected by this min or application?		
Minor app #1	<input type="checkbox"/> Does this minor application store PII?	
	If yes, where?	
	Who has access to this data?	

Name	Description	Comments
<input type="checkbox"/> Is PII collected by this min or application?		
Minor app #2	<input type="checkbox"/> Does this minor application store PII?	
	If yes, where?	
	Who has access to this data?	

Name	Description	Comments
<input type="checkbox"/> Is PII collected by this min or application?		
Minor app #3	<input type="checkbox"/> Does this minor application store PII?	
	If yes, where?	
	Who has access to this data?	

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.

Minor app #1	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?				

Minor app #2	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?				

Minor app #3	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?				

---

OUTPATIENT PHARMACY	SOCIAL WORK
PAID	SPINAL CORD DYSFUNCTION
PATCH MODULE	SURGERY
PATIENT DATA EXCHANGE	SURVEY GENERATOR
PATIENT FEEDBACK	TEXT INTEGRATION UTILITIES
PATIENT REPRESENTATIVE	TOOLKIT
PCE PATIENT CARE	UNWINDER
ENCOUNTER	UTILIZATION MANAGEMENT ROLLUP
PCE PATIENT/IHS SUBSET	UTILIZATION REVIEW
PHARMACY BENEFITS	VA CERTIFIED COMPONENTS - DSSI
MANAGEMENT	VA FILEMAN
PHARMACY DATA	VBECS
MANAGEMENT	VDEF
PHARMACY NATIONAL	VENDOR - DOCUMENT STORAGE SYS
DATABASE	VHS&RA ADP TRACKING SYSTEM
PHARMACY PRESCRIPTION	VISIT TRACKING
PRACTICE	VISTALINK
POLICE & SECURITY	VISTALINK SECURITY
PROBLEM LIST	VISUAL IMPAIRMENT SERVICE TEAM
PROGRESS NOTES	ANRV
PROSTHETICS	VOLUNTARY TIMEKEEPING
QUALITY ASSURANCE	VOLUNTARY TIMEKEEPING NATIONAL
INTEGRATION	WOMEN'S HEALTH
QUALITY IMPROVEMENT	CARE TRACKER
CHECKLIST	
QUASAR	
RADIOLOGY/NUCLEAR	
MEDICINE	
RECORD TRACKING	
REGISTRATION	
RELEASE OF INFORMATION - DSSI	
REMOTE ORDER/ENTRY	
SYSTEM	
RPC BROKER	
RUN TIME LIBRARY	
SAGG	
SCHEDULING	
SECURITY SUITE UTILITY PACK	
SHIFT CHANGE HANDOFF	
TOOL	

(FY 2010) PIA: Minor Applications

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

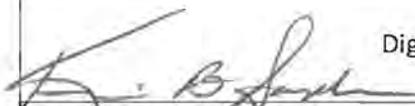
Name	Description	Comments
N/A		
<input type="checkbox"/> Is PII collected by this min or application?		
Minor app #1	<input type="checkbox"/> Does this minor application store PII?	
	If yes, where?	
	Who has access to this data?	

Name	Description	Comments
<input type="checkbox"/> Is PII collected by this min or application?		
Minor app #2	<input type="checkbox"/> Does this minor application store PII?	
	If yes, where?	
	Who has access to this data?	

Name	Description	Comments
<input type="checkbox"/> Is PII collected by this min or application?		
Minor app #3	<input type="checkbox"/> Does this minor application store PII?	
	If yes, where?	
	Who has access to this data?	

### (FY 2010) PIA: Final Signatures

Facility Name: Harry S Truman Memorial Veterans Hospital

Title	Name	Phone	Email
Privacy Officer:	Ann Richmond	573-814-6589	ann.richmond@va.gov
 Digital Signature Block 3-19-10			
Information Security Officer:	Kevin Sample	573-814-6250	kevin.sample@va.gov
 Digital Signature Block 3/19/10			
Chief Information Officer:	Donna Krause	573-814-6501	donna.krause@va.gov
 Digital Signature Block 3-19-10			
Person Completing Document:	All designees listed above	0	0
Digital Signature Block			
System / Application / Program Manager:		0	0
Digital Signature Block			

Date of Report: 3/1/2010  
 OMB Unique Project Identifier: 029-00-02-00-01-1120-00  
 Project Name: REGION 2 > VHA > VISN 15 > Columbia VAMC > LAN