

(FY 2010) PIA: System Identification

Program or System Name: REGION 1 > VHA > VISN 19 > Grand Junction VAMC > LAN

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

Description of System / Application / Program:

The Grand Junction VA Medical Center's Local Area Network (LAN) is comprised of a core switch, approximately two dozen distribution switches, a Dynamic Host Communication Protocol (DHCP) server and utility servers. Inter-switch connectivity is through multi-mode fiber optic cables. Approximately 600 PC Workstations are connected to the distribution switches through Category 5 or Category 5e cable (4 pair, 24 awg). Additional connections include a small Wireless Network, supported through an Air Fortress (FIPS 140-2 certified) Wireless gateway, providing primary support to the VA's Bar Code Medicine Administration (BCMA) initiative [areas 3P, 3MS, 5MS, Ambulatory Care, CLC & ER] and connections to three outlying VA clinics. There are 4 Routers, 38 switches and 23 Signal closets.

Facility Name: Grand Junction VAMC

Title:	Name:	Phone:	Email:
Privacy Officer:	Margaret Grunow	970 263-5021	Margaret.Grunow@va.gov
Information Security Officer:	Phil Olson	970 263-5013	Phil.Olson@va.gov
Chief Information Officer:	Roman Black	970 263-5093	Roman.Black@va.gov
Person Completing Document:	Margaret Grunow	970 263-5021	Margaret.Grunow@va.gov
System Manager	Roman Black	970 263-5093	Roman.Black@va.gov

Other Titles:

Other Titles:

Date of Last PIA Approved by VACO Privacy

Services: (MM/YYYY)

05/2008

Date Approval To Operate Expires:

11/2011

What specific legal authorities authorize this program or system:	Title 38, United States Code, Section 7301
What is the expected number of individuals that will have their PII stored in this system:	15,000 to 30,000
Identify what stage the System / Application / Program is at:	Operations/Maintenance
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.	Operational since 11/1998 11 years 3 months
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):	02/2010

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?

No

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):
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)?

Does the System of Records Notice require modification or updating?

(Please Select Yes/No)

Is PII collected by paper methods?	No	
Is PII collected by verbal methods?	No	
Is PII collected by automated methods?	No	
Is a Privacy notice provided?	No	N/A
Proximity and Timing: Is the privacy notice provided at the time of data collection?	No	N/A
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	No	N/A
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	No	N/A
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	No	N/A

(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)	N/A	N/A	N/A	N/A
Family Relation (spouse, children, parents, grandparents, etc)	N/A	N/A	N/A	N/A
Service Information	N/A	N/A	N/A	N/A
Medical Information	N/A	N/A	N/A	N/A
Criminal Record Information	N/A	N/A	N/A	N/A
Guardian Information	N/A	N/A	N/A	N/A
Education Information	N/A	N/A	N/A	N/A
Benefit Information	N/A	N/A	N/A	N/A
Other (Explain)				

PII is not collected by this system but is stored as part of correspondence, reports, and various other administrative functions as it relates to Veteran Health Care

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)	No	No	No	
Family Relation (spouse, children, parents, grandparents, etc)	No	No	No	
Service Information	No	No	No	
Medical Information	No	No	No	
Criminal Record Information	No	No	No	
Guardian Information	No	No	No	
Education Information	No	No	No	

Benefit Information	No	No	No
Other (Explain)			
Other (Explain)			
Other (Explain)			

PII is not collected by this system but is stored as part of correspondence, reports, and various other administrative functions as it relates to Veteran Health Care

(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	N/A	No	N/A	N/A	
Other Veteran Organization	N/A	No	N/A	N/A	
Other Federal Government Agency	N/A	No	N/A	N/A	
State Government Agency	N/A	No	N/A	N/A	
Local Government Agency	N/A	No	N/A	N/A	
Research Entity	N/A	No	N/A	N/A	
Other Project / System	VA Files and Databases: PII may be found in administrative correspondence, reports, and other administrative action, related to Veteran Health Care, from VISTA (collected and stored a				
Other Project / System	Other information: The LAN does not collect or store PII of any kind, but incidental or secondary PII could be stored under folders for the specific services. This would be administrative health care, eligibility, medical care cost recovery, employee or information received for the purpose of treatment related.				

(FY 2010) PIA: Access to Records

Does the system gather information from another system? No

Please enter the name of the system: N/A

Per responses in Tab 4, does the system gather information from an individual? No

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?

No

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

if yes, please check all that apply:

Describe process for authorizing access to this data.

N.A.

Answer:

[Redacted]

at the RDPC in Denver), Austin Databases, Cancer Registry, Organ Donation, Transplant List and other VA Organizations (such as VBA, HEC, OPM

[Redacted]

[Redacted]

(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:

There is no inspection of user home directories

Answer:

How is data checked for completeness?

N/A

Answer:

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

N/A

Answer:

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

N/A

Answer:

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

Answer:

The LAN system is just a transport mechanism, it doesn't store or collect any data

(FY 2010) PIA: Retention & Disposal

What is the data retention period?

Answer:

N/A

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

Answer:

N/A

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

Answer:

N/A

Where are these procedures documented?

Answer:

N/A

How are data retention procedures enforced?

Answer:

N/A

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 Access to the LAN provides the path to the information, authorization or security is implemented by Network Port Security

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 Security monitoring is constantly performed at the regional and national levels

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: The LAN System Security Plan (SSP) is based on NIST 800-53, Clinger Cohen act

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 checked="" 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 type="checkbox"/> Cold/Frost/Snow | <input checked="" type="checkbox"/> Sabotage/Terrorism |
| <input checked="" type="checkbox"/> Communications Loss | <input 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 type="checkbox"/> Earthquakes | <input checked="" type="checkbox"/> Burglary/Break In/Robbery |
| <input checked="" 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: The LAN does not store or collect information

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?

YES

Please add additional controls:

0	FALSE	High
0	FALSE	Moderate
1	TRUE	Low

20	TRUE	High
0	FALSE	Moderate
0	FALSE	Low

0	FALSE	High
5	TRUE	Moderate
0	FALSE	Low
26	Total	

The ultimate objective is to conduct the day-to-day operations of the VA and to accomplish our stated mission with what the Office of Management and Budget (OMB) Circular A-130 defines as adequate security including the magnitude of harm to individuals, the VA, or its assets resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow NIST SP800-53 low impact defined set of controls.

Low

The VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow NIST SP800-53 moderate impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of this facility/ common security controls. These issues are identified and described in the system security plans for the individual information systems.

Med

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.

High

Security
awareness
training
to inform
personnel
including
contractors and
other
users of
information
systems
that
support
our
operations and
assets of
the
information
security
risks
associated with
their

(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)

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) Record Interchange (CAPRI)	Purchase Order Management System (POMS)	
Web Service Medical Records (WebSMR)	Control of Veterans Records (COVERS)	Veterans Canteen Web	
Systematic Technical Accuracy Review (STAR)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)	Inventory Management System (IMS)	
Fiduciary STAR Case Review	Fiduciary Beneficiary System (FBS)	Synquest	
Veterans Exam Request Info System (VERIS)	Hearing Officer Letters and Reports System (HOLAR)	RAI/MDS	x
Web Automated Folder Processing System (WAFPS)	Inforce	ASSISTS	x
Courseware Delivery System (CDS)	Awards	MUSE	x
Electronic Performance Support System (EPSS)	Actuarial	Bbraun (CP Hemo)	
Veterans Service Representative (VSR) Advisor	Insurance Self Service	VIC	x
Loan Guaranty Training Website	Insurance Unclaimed Liabilities	BCMA Contingency Machines	x
C&P Training Website	Insurance Online	Script Pro	x

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

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

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

Baker System		Veterans Assistance Discharge System (VADS)
Dental Records Manager	x	VBA Training Academy
Sidexis		Veterans Service Network (VETSNET) Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
Priv Plus	x	BIRLS
Mental Health Assistant		Centralized Accounts Receivable System (CARS)
Telecare Record Manager		
Omnicell	x	Compensation & Pension (C&P)
Powerscribe Dictation System		Corporate Database
EndoSoft		Control of Veterans Records (COVERS)
Compensation and Pension (C&P)		Data Warehouse
Montgomery GI Bill		INS - BIRLS
Vocational Rehabilitation & Employment (VR&E) CH 31		Mobilization
Post Vietnam Era educational Program (VEAP) CH 32		Master Veterans Record (MVR)
Spinal Bifida Program Ch 18		BDN Payment History
C&P Payment System		
Survivors and Dependents Education Assistance CH 35		
Reinstatement Entitlement Program for Survivors (REAPS)		
Educational Assistance for Members of the Selected Reserve Program CH 1606		
Reserve Educational Assistance Program CH 1607		
Compensation & Pension Training Website		
Web-Enabled Approval Management System (WEAMS)		
FOCAS		
Work Study Management System (WSMS)		
Benefits Delivery Network (BDN)		
Personnel and Accounting Integrated Data and Fee Basis (PAID)		
Personnel Information Exchange System (PIES)		
Rating Board Automation 2000 (RBA2000)		
SHARE		
Service Member Records Tracking System		

(FY 2010) PIA: VISTA Minor Applications

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

ACCOUNTS RECEIVABLE	DRUG ACCOUNTABILITY	INPATIENT MEDICATIONS
ADP PLANNING (PLANMAN)	DSS EXTRACTS	INTAKE/OUTPUT
ADVERSE REACTION TRACKING	EDUCATION TRACKING	INTEGRATED BILLING
ASISTS	EEO COMPLAINT TRACKING	INTEGRATED PATIENT FUNDS
AUTHORIZATION/SUBSCRIPTION	ELECTRONIC SIGNATURE	INTERIM MANAGEMENT
AUTO REPLENISHMENT/WARD STOCK	ENGINEERING	SUPPORT
AUTOMATED INFO COLLECTION SYS	ENROLLMENT APPLICATION	KERNEL
AUTOMATED LAB INSTRUMENTS	SYSTEM	KIDS
AUTOMATED MED INFO EXCHANGE	EQUIPMENT/TURN-IN	LAB SERVICE
BAR CODE MED ADMIN	REQUEST	LETTERMAN
BED CONTROL	EVENT CAPTURE	LEXICON UTILITY
BENEFICIARY TRAVEL	EVENT DRIVEN REPORTING	LIBRARY
CAPACITY MANAGEMENT - RUM	EXTENSIBLE EDITOR	LIST MANAGER
CAPRI	EXTERNAL PEER REVIEW	MAILMAN
CAPACITY MANAGEMENT TOOLS	FEE BASIS	MASTER PATIENT INDEX
CARE MANAGEMENT	FUNCTIONAL	VISTA
CLINICAL CASE REGISTRIES	INDEPENDENCE	MCCR NATIONAL
CLINICAL INFO RESOURCE NETWORK	GEN. MED. REC. - GENERATOR	DATABASE
CLINICAL MONITORING SYSTEM	GEN. MED. REC. - I/O	MEDICINE
CLINICAL PROCEDURES	GEN. MED. REC. - VITALS	MENTAL HEALTH
CLINICAL REMINDERS	GENERIC CODE SHEET	MICOM
CMOP	GRECC	MINIMAL PATIENT
CONSULT/REQUEST TRACKING	HEALTH DATA &	DATASET
CONTROLLED SUBSTANCES	INFORMATICS	MYHEALTHVET
CPT/HCPCS CODES	HEALTH LEVEL SEVEN	Missing Patient Reg (Original)
CREDENTIALS TRACKING	HEALTH SUMMARY	A4EL
DENTAL	HINQ	NATIONAL DRUG FILE
DIETETICS	HOSPITAL BASED HOME	NATIONAL LABORATORY
DISCHARGE SUMMARY	CARE	TEST
DRG GROUPER	ICR - IMMUNOLOGY CASE	NDBI
	REGISTRY	NETWORK HEALTH
	IFCAP	EXCHANGE
	IMAGING	NOIS
	INCIDENT REPORTING	NURSING SERVICE
	INCOME VERIFICATION MATCH	OCCURRENCE SCREEN
	INCOMPLETE RECORDS	ONCOLOGY
	TRACKING	ORDER ENTRY/RESULTS
		REPORTING

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

Minor app #1

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

Minor app #2

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

Minor app #3

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 ENCOUNTER	UNWINDER
PCE PATIENT/IHS SUBSET	UTILIZATION MANAGEMENT ROLLUP
PHARMACY BENEFITS MANAGEMENT	UTILIZATION REVIEW
PHARMACY DATA MANAGEMENT	VA CERTIFIED COMPONENTS - DSSI
PHARMACY NATIONAL DATABASE	VA FILEMAN
PHARMACY PRESCRIPTION PRACTICE	VBECs
POLICE & SECURITY	VDEF
PROBLEM LIST	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES	VHS&RA ADP TRACKING SYSTEM
PROSTHETICS	VISIT TRACKING
QUALITY ASSURANCE INTEGRATION	VISTALINK
QUALITY IMPROVEMENT CHECKLIST	VISTALINK SECURITY
QUASAR	VISUAL IMPAIRMENT SERVICE TEAM ANRV
RADIOLOGY/NUCLEAR MEDICINE	VOLUNTARY TIMEKEEPING
RECORD TRACKING	VOLUNTARY TIMEKEEPING NATIONAL
REGISTRATION	WOMEN'S HEALTH
RELEASE OF INFORMATION - DSSI	CARE TRACKER
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.

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

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

Minor app #3	Name		Description	Comments
		<input type="checkbox"/>	Is PII collected by this min or application?	
		<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: Grand Junction VA MC

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

Privacy Officer:	Margaret Grunow	970 263-5021	Margaret.Grunow@va.gov
------------------	-----------------	--------------	------------------------



Margaret A. Grunow 3-31-2010

Information Security Officer:	Phil Olson	970 263-5013	Phil.Olson@va.gov
-------------------------------	------------	--------------	-------------------



Chief Information Officer:	Roman Black	970 263-5093	Roman.Black@va.gov
----------------------------	-------------	--------------	--------------------



Person Completing Document:	Margaret Grunow	970 263-5021	Margaret.Grunow@va.gov
-----------------------------	-----------------	--------------	------------------------

Margaret A. Gueon 3-31-2010

System / Application / Program Manager: Roman Black 970 263-5093 Roman.Black@va.gov

Date of Report: 2/19/2010
OMB Unique Project Identifier 029-00-02-00-01-1120-00
Project Name REGION 1 > VHA > VISN 19 > Grand Junction VAMC > LAN

0

The Signature Process:

- Complete the PIA form.
- Name the PIA Excel FORM ["FY09-Region # - Facility Name - Facility # -Date(mmddyyyy).xls"]
 - Example: "FY09-Region3-Lexington VAMC-596-10302008.xls"
- Submit the completed PIA Excel form to SMART Database.
- Fix errors the reviewers sent back, rename the file and submit to SMART Database
- If no errors, convert form into PDF with Nuance PDF Professional.
- Name the PIA PDF form ["FY09-Region #-Facility Name- Facility # -Date(mmddyyyy).xls"]
- Remove the Security Tab ****Will not be published!****
- Obtain digital signatures on the "Final Signatures tab"