

Welcome to the PIA for FY 2011!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

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

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 referenced in the procedure section of this document.

- a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Directive 6508.
- b. Records Officer is responsible for supplying records retention and deletion schedules.
- c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Directive 6508 and to immediately report all anomalies to the Privacy Service and appropriate management chain.
- d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.
- e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

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

Macros Must Be Enabled on This Form

Microsoft Office 2003: To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

Microsoft Office 2007: To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable All Macros; 2) Click OK

Final Signatures

Final Signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.

Privacy Impact Assessment Uploaded into SMART

Identification

Program or System Name: REGION 3>VHA>VISN
06>SALEM VAMC>LAN

Identifier (AKA: UPID #): 029-00-02-00-01-1120-00

Description of System/ Application/ Program: The SALEM VAMC uses the Local Area Network (LAN) as a General Support System, supporting mission-critical and other systems necessary to conduct day-to-day operations within the Veterans Health Administration. Applications and devices within the LAN support numerous areas, including medical imaging, supply management, decision support, medical research, and education.

Facility Name: Salem VAMC

Title:	Name:	Phone:	Email:
Privacy Officer:	Robert A. Bidwell	540.855.5050	robert.bidwell1@va.gov
Information Security Officer:	Valarie Hoover	540.855.3457	valarie.hoover@va.gov
System Owner/ Chief Information Officer:	Sharon Collins	540.982.2463x2604	sharon.collins@va.gov
Information Owner:	James Belinfontie	540.982.2463x3324	james.belinfontie@va.gov
Other Titles:			

Person Completing Document: Robert A. Bidwell

Other Titles:

Services: (MM/YYYY) 02.28.2010

Date Approval To Operate Expires: 04.30.2011

What specific legal authorities authorize this program or system: Title 38, United States Code, Section 7301(a); Department of Veterans Affairs Act PL 100-527 of 1988 and PL 104-191, 110 Statute 1936, and FIPS 199 and FIPS 200

What is the expected number of individuals that Program is at: 1 to 9,900,000 Operations/Maintenance

The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number Since 1994

Is there an authorized change control process which documents any changes to existing

If No, please explain:

Has a PIA been completed within the last three years?

Date of Report (MM/YYYY): 04/2011

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 |
| 2. Name of the System of Records: | Patient Medical Records |
| 3. Location where the specific applicable System of Records Notice may be accessed (include the URL): | http://www.ofr.gov/Privacy/2009 |

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

Does the System of Records Notice require modification or updating? No

(Please Select Yes/No)

Is PII collected by paper methods? Yes

Is PII collected by verbal methods? Yes

Is PII collected by automated methods? Yes

Is a Privacy notice provided? Yes

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

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

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

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

(FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Verbal	Health care	Verbally	Verbally
Family Relation (spouse, children, parents, grandparents, etc)	VA File Database	Health care	Written	Written
Service Information	Electronic/File Transfer	Benefits	Verbal & Written	Verbal & Written
Medical Information	VA File Database	Health care	Verbal & Written	Written
Criminal Record Information				
Guardian Information	Paper	Health care	Written	Written
Education Information	Verbal	Research	Verbally	Verbally
Benefit Information	Paper	Benefits	Written	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	VA Files / Databases (Identify file)	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory	

Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory
Criminal Record Information	No	VA Files / Databases (Identify file)	Mandatory
Guardian 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)			

(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	VBA	Yes	Income verification, C&P Exam information, tort claim feasons and death notifications	Both PII & PHI	1605.145 CFR 164.500 thru 164.534 - VHA 1605.1 and VHA 1605.2
Other Veteran Organization					
Other Federal Government Agency	DoD, CDC, HHS	Yes	DoD for treatment, CDC for tracking communicable diseases, HHS for action if abuse is found	Both PII & PHI	1605.145 CFR 164.500 thru 164.534 - VHA 1605.1 and VHA 1605.2
State Government Agency	Virginia Veterans Care Center	No	Health care coordination	Both PII & PHI	1605.145 CFR 164.500 thru 164.534 - VHA 1605.1 and VHA 1605.2
Local Government Agency	City and County Health Departments	No	Reportable disease reporting	Both PII & PHI	1605.145 CFR 164.500 thru 164.534 - VHA 1605.1 and VHA 1605.2
Research Entity	Salem Research Institute	No	Information per approved research protocols	Both PII & PHI	1605.145 CFR 164.500 thru 164.534 - VHA 1605.1 and VHA 1605.2
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system? Yes
 Please enter the name of the system: Re-Pricer and Patient reminder notifications 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? 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.

Answer: VHA Handbook 1605.1 and VHA Handbook 1605.2

(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: Information collected are directed by VHA Directives. The Directives provide guidance on the information needed to provide care to patients. The Web form is located at <https://www.1010EZ.med.va.gov/sec/vah/1010EZ>.

How is data checked for completeness?

Answer: Information may be verified by written documentation provided by Veterans, by DoD data base, SSA, and/or VBA data.

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

Answer: Means tests are performed annually to verify that information is current. Occasionally written documents may be requested to verify information.

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

Answer: New information may be verified by SSA, DoD, VBA and other agency data uses.

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: 75 years from the last date of activity.

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

Answer: Health care operations

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

Answer: Retirement of the records in accordance with RCS 10-1

Where are these procedures documented?

Answer: RCS 10-1 and Medical Center Policies

How are data retention procedures enforced?

Answer: Reviews by the Records Manager

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: N/A

(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: The agency is following IT security requirements as described in the FISMA. IT security is provided at the project and enterprise levels. IT security measures included the use of passwords, user authentication, physical security controls and configuration management. Enterprise level IT security includes firewalls for intrusion protection, virus protection software, and the implementation of authentication systems. Risk assessments are conducted. VA OI&T Field Security Service provides policy or NIST guidelines. VA OI&T Field Security Service will serve as a point of contact for additional questions or specifics on implementation of security measures. At the Department level the CIO's Office, VA OI&T Field Security Service is responsible for the establishment of directives, policies, & procedures which are consistent with the provisions of Federal Information Security Management Act (FISMA) as well as guidance issued by the Office of Management & Budget (OMB), the National Institute of Standards & Technology (NIST), & other requirements that Vista-Legacy is and has been subject to. In addition, VA OI&T Field Security Service administers and manages Department-wide security solutions.

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 checked="" 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"/> Storms/Hurricanes |

7. Security

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

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

- Storms/Hurricanes
- Substance Abuse
- Theft of Assets
- Theft of Data
- Vandalism/Rioting

Answer: (Other Risks)

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

- | | | |
|--|---|---|
| <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.

Answer:

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)

- | | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | 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. |
| <input type="checkbox"/> | The potential impact is moderate 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 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)

- | | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | 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. |
| <input type="checkbox"/> | The potential impact is moderate 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 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)

- | | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | 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. |
| <input type="checkbox"/> | The potential impact is moderate 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 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.

During the course of completing this assessment, in multiple instances we have indicated that the LAN is not intended to be used for retention or storage of PII. The Network Administrators are unable to restrict or monitor the retention or storage of information by all system users. It is assumed that some users are retaining or storing PII on components of the LAN during the course of business.

Users are able to create their own .PST files and personal folders on the LAN. PII may be included in emails and documents stored in these files and folders by individual users.

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?
--

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

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

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

Web Automated Folder Processing System (WAFPS)
Web Automated Reference Material System (WARMS)
Web Automated Verification of Enrollment
Web-Enabled Approval Management System (WEAMS)
Web Service Medical Records (WebSMR)
Work Study Management System (WSMS)

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

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

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: Minor Applications

Which of these are sub-components of your system?

1184 Web A4P	ENDSOFT Enterprise Terminology Server & VHA Enterprise Terminology Services	RAFT RALS
Administrative Data Repository (ADR) ADT	ePROMISE	X Remedy Application
Agent Cashier	EYECAP	X SAN
X Air Fortress	Financial and Accounting System (FAS)	Scanning Exam and Evaluation System
Auto Instrument	Financial Management System	X Sentillion
Automated Access Request	Genesys	Stellant
X BDN 301	X Health Summary Contingency	X Stentor
	ICB	Tracking Continuing Education
X Bed Board Management System	KOWA	Traumatic Brain Injury
Cardiff Teleform	Lynx Duress Alarm	VA Conference Room Registration VAMedSafe
X Cardiology Systems (stand alone servers from the network)	MHTP	
CHECKPOINT	X Microsoft Active Directory	VBA Data Warehouse
X Clinical Data Repository/Health Data Repository	X Microsoft Exchange E-mail System	VHAHUNAPP1
Combat Veteran Outreach Committee on Waiver and Compromises	Military/Vet Eye Injury Registry	VHAHUNFPC1
X CP&E	X Mumps AudioFAX	X VISTA RAD
X Crystal Reports Enterprise	NOAHLINK	Whiteboard
X Data Innovations	X Omnicell	
DELIVEREX	Onvicord (VLOG)	
X DICTATION-Power Scribe	Optifill	
DRM Plus	P2000 ROBOT	
DSIT	PACS database	
X DSS Quadramed	Personal Computer Generated Letters	
X EDS Whiteboard (AVJED)	PICIS OR	
X EKG System	X PIV Systems	
Embedded Fragment Registry	Q-Matic	
	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	Precision Links/Co-Pilot
Description	Diabetic monitoring and assessments
Comments	
Is PII collected by this minor application?	Yes
Does this minor application store PII?	Yes
If yes, where?	PII is Stored in a restricted access folder, within the Service folder on the public drive
Who has access to this data?	Specified staff in Primary Care

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 3>VHA>VISN 06>SALEM VAMC>LAN

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

Privacy Officer:	Robert A. Bidwell	540.855.5050	robert.bidwell1@va.gov
------------------	-------------------	--------------	------------------------

--

Information Security Officer:	Valarie Hoover	540.855.3457	valarie.hoover@va.gov
-------------------------------	----------------	--------------	-----------------------

--

System Owner/ Chief Information Officer:	Sharon Collins	540.982.2463x2604	sharon.collins@va.gov
--	----------------	-------------------	-----------------------

--

Information Owner:	James Belinfontie	540.982.2463x3324	james.belinfontie@va.gov
--------------------	-------------------	-------------------	--------------------------

--

Other Titles:

--

Date of Report: #REF!

OMB Unique Project Identifier 0

Project Name REGION 3>VHA>VISN 06>SALEM VAMC>LAN

The Signature Process:

- Complete the PIA form.
- Name the PIA Excel FORM ["FY11-Region # - Facility Name - Facility # -Date(mmddyyyy).xls"]
 - Example: "FY11-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 ["FY11-Region #-Facility Name- Facility # -Date(mmddyyyy).xls"]
- Remove the Security Tab **Will not be published!**
- Obtain digital signatures on the "Final Signatures tab"