

## **Welcome to the PIA for FY 2011!**

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

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

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

### **Directions:**

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

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

PIA Website: [http://vawww.privacy.va.gov/Privacy\\_Impact\\_Assessments.asp](http://vawww.privacy.va.gov/Privacy_Impact_Assessments.asp)

### **Roles and Responsibilities:**

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

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

### **Definition of PII (Personally Identifiable Information)**

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

### **Macros Must Be Enabled on This Form**

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

**Microsoft Office 2007:** To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable

All Macros; 2) Click OK

**Final Signatures**

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

**Privacy Impact Assessment Uploaded into SMART**

Privacy Impact Assessments should be uploaded into C&A section of SMART.

All PIA Validation Letters should be emailed to [christina.pettit@va.gov](mailto:christina.pettit@va.gov) to received full credit for submission.

## (FY 2011) PIA: System Identification

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

Description of System/ Application/ Program: Each VA facility 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: G. V. (Sonny) Montgomery VA Medical Center, Jackson, MS

Title:	Name:	Phone:	Email:
Privacy Officer:	Aletia Arbuthnot	601-362-4471	<a href="mailto:aletia.arbuthnot@va.gov">aletia.arbuthnot@va.gov</a>
Information Security Officer:	Lance Boyington	601-362-4471	<a href="mailto:lance.boyington@va.gov">lance.boyington@va.gov</a>
System Owner/ Chief Information Officer:	Dale Nelson for BK Hack	479-587-5886	<a href="mailto:Riley.nelson@va.gov">Riley.nelson@va.gov</a>
Information Owner:	Julie Catellier	601-362-4471	<a href="mailto:Julie.Cateillier@va.gov">Julie.Cateillier@va.gov</a>
Other Titles:	Robert Wolak	601-364-1385	<a href="mailto:robert.wolak@va.gov">robert.wolak@va.gov</a>

Person Completing Document: Evan M. Jones 601-368-3995 [evan.jones2@va.gov](mailto:evan.jones2@va.gov)

Other Titles:

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

Date Approval To Operate Expires: 08/2011

What specific legal authorities authorize this program or system: Title 38, United States Code, section 7301(a); Title 38, United States Code, Sections 501(b) and 304.

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

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. 17 years

Is there an authorized change control process which documents any changes to existing applications or systems? Yes

If No, please explain:

Has a PIA been completed within the last three years? Yes

Date of Report (MM/YYYY): 05/2011

**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?

- 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 2 & TAB 12. ( See Comment for Definition of PII)**

## (FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.

Yes

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

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

79VA19; 24VA19

2. Name of the System of Records:

Veterans Health Information Systems and Technology Architecture (VistA) Records-VA; Patient Medical Records-VA (Formally known as 24VA136)-VA

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

[http://www.rms.oit.va.gov/SOR\\_Records.asp](http://www.rms.oit.va.gov/SOR_Records.asp)

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

Yes

Does the System of Records Notice require modification or updating?

No

***(Please Select Yes/No)***

Is PII collected by paper methods?

Yes

Is PII collected by verbal methods?

Yes

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

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.

<b>Data Type</b>	<b>Collection Method</b>	<b>What will the subjects be told about the information collection?</b>	<b>How is this message conveyed to them?</b>	<b>How is a privacy notice provided?</b>
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Verbal	The information is used to treat and care for the veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of the veteran.	Verbally	Verbally
Family Relation (spouse, children, parents, grandparents, etc)	VA File Database	for the veteran patient. Clinical information from VA and DoD is used in	Written	Written
Service Information	Electronic/File Transfer	The information is used to treat and care for the veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of the veteran.	Verbally	Written
Medical Information	Paper	The information is used to treat and care for the veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of the veteran.	Written	Written
Criminal Record Information	Electronic/File Transfer	The information is used to treat and care for the veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of the veteran.	Verbally	Written
Guardian Information	Electronic/File Transfer	The information is used to treat and care for the veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of the veteran.	Verbally	Written

Education Information	Electronic/File Transfer	The information is used to treat and care for the veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of the veteran.	Verbally	Written
Benefit Information	Electronic/File Transfer	The information is used to treat and care for the veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of the veteran.	Verbally	Written
Other (Explain)		N/A		

<b>Data Type</b>	<b>Is Data Type Stored on your system?</b>	<b>Source</b> (If requested, identify the specific file, entity and/or name of agency)	<b>Is data collection Mandatory or Voluntary?</b>	<b>Additional Comments</b>
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Mandatory	
Service Information	Yes	Veteran	Mandatory	
Medical Information	Yes	Veteran	Mandatory	
Criminal Record Information	Yes	Veteran	Mandatory	
Guardian Information	Yes	Veteran	Mandatory	
Education Information	No			
Benefit Information	Yes	Veteran	Mandatory	
Other (Explain)				
Other (Explain)				

Other (Explain)

---

(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization					
Other Veteran Organization	State Veterans Home	Yes	PII and PHI for continuity of Care	Both PII & PHI	VA 6500
Other Federal Government Agency					
State Government Agency					
Local Government Agency					
Research Entity					
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:	DoD	
Per responses in Tab 4, does the system gather information from an individual?		Yes
If information is gathered from an individual, is the information provided:	<input checked="" type="checkbox"/> Through a Written Request <input checked="" type="checkbox"/> Submitted in Person <input checked="" type="checkbox"/> Online via Electronic Form	
Is there a contingency plan in place to process information when the system is down?		Yes

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?		Yes
if yes, please check all that apply:	<input checked="" type="checkbox"/> Drug/Alcohol Counseling <input checked="" type="checkbox"/> Mental Health <input type="checkbox"/> HIV <input checked="" type="checkbox"/> Research <input type="checkbox"/> Sickle Cell <input type="checkbox"/> Other (Please Explain)	
Describe process for authorizing access to this data.		
Answer: <b>Access request are processed through the ISO and OI&amp;T following VA 6500 and NIST Guidelines</b>		

## (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: **Data is collected electronically based on the automation of VA forms and clinical procedures.**

How is data checked for completeness?

Answer: **Data is reviewed by staff and compared to paper forms.**

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

Answer: **Clinical data is removed. Administrative data is updated with each application for care.**

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

Answer: **New data is compared with printed form or via patient verification.**

*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 after patient last episode.**

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

Answer: **The data is needed in order to ensure on going quality of care, as well as verification of continued eligibility.**

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

Answer: **Applicable federal regulatory requirements will be followed for eliminating or disposing of data. For example paper documents will be shredded while electronic media will be wiped and shredded to meet applicable federal regulatory requirements.**

Where are these procedures documented?

Answer: **VA Handbook 6300; Record Control Schedule 10-1**

How are data retention procedures enforced?

Answer: **Procedures will be enforced sing technical and managerial control mechanism.**

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

Yes

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

Answer:

## (FY 2011) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?

No

If Yes, How will parental or guardian approval be obtained?

Answer:

---

## (FY 2011) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured. Yes

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.. Yes

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

If 'No' to any of the 3 questions above, please describe why:

Answer:

Is adequate physical security in place to protect against unauthorized access? Yes

If 'No' please describe why:

Answer:

Explain how the project meets IT security requirements and procedures required by federal law.

Answer: **Review of privacy notice, data protection methods and review security controls.**

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

Answer: (Other Risks)

---

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

- Access Control
- Contingency Planning
- Personnel Security
- Audit and Accountability
- Identification and Authentication
- Physical and Environmental Protection
- Awareness and Training
- Incident Response
- Risk Management
- Certification and Accreditation Security Assessments
- Configuration Management
- 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: **Review of privacy notice, data protection methods and review security controls.**

---

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization?  
**(Choose One)**

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

Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?  
**(Choose One)**

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

Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? **(Choose One)**

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

---

The controls are being considered for the project based on the selections from the previous assessments?

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

---

*Please add additional controls:*

---

**(FY 2011) PIA: Additional Comments**

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

## (FY 2011) PIA: VBA Minor Applications

<b>Which of these are sub-components of your system?</b>
--

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

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

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

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

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

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

(FY 2011) PIA: Minor Applications

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

1184 Web	ENDSOFT	RAFT
A4P	Enterprise Terminology Server & VHA Enterprise Terminology Services	RALS

# (FY 2011) PIA: Final Signatures

Facility Name: Region 2>VHA>VISN 16>Jackson VAMC> LAN

Privacy Officer: Aletia Arbuthnot 601-362-4471

Digital Signature Block  8 June 2011

Information Security Officer: Lance Boyington 601-362-4471

Digital Signature Block  8 June 2011

System Owner/ Chief Information Officer: Dale Nelson for BK Hack 479-587-5886

Digital Signature Block

Information Owner: Julie Catellier 601-362-4471

Digital Signature Block  JUN 08 2011

Other Titles: Robert Wolak 601-364-1385

Digital Signature Block  8 Jun 2011

Date of Report: 5/13/11

OMB Unique Project Identifier 029-00-02-00-01-1120-00

Project Name Region 2>VHA>VISN 16>Jackson VAMC> LAN

Email:

aletia.arbutnot@va.gov

lance.boyington@va.gov

Riley.nelson@va.gov

Julie.Cateillier@va.gov

robert.wolak@va.gov