

(FY 2011) PIA: System Identification

Program or System Name: REGION 3 > VHA > VISN 06 > Hampton VAMC > LAN
OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-02-00-01-1120-00

Description of System/ Application/ Program: This is the group of switches, servers and workstations connected by fiber optic cable that comprises the Hampton VA Medical Center local area network. The network provides a backbone which allows connectivity to the VistA Cluster housing the VistA application and database, provides Microsoft Office applications and stores files created using these and other applications. Printing capabilities for these files and databases is also provided by the LAN. Email using MS Outlook/Exchange is also provided via the LAN.

Facility Name: Hampton VA Medical Center

Title:	Name:	Phone:	Email:
Privacy Officer:	Lisa Wright (Acting)	757-722-9961 x-1679	lisa.wright@va.gov
Information Security Officer:	Timothy Brooks	757-722-9961 x-2584	timothy.brooks@va.gov
System Owner/ Delegation of Authority	Kevin Marlowe	757-722-9961 x-2566	kevin.marlowe@va.gov
Network Information Security Officer:	Steven Blackwell	757-722-9961 x-7722	steven.blackwell@va.gov
Other Titles:			

Person Completing Document: Steven Blackwell

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY) 12/2007

Date Approval To Operate Expires: 08/2011

What specific legal authorities authorize this program or system: Title 38 USC

What is the expected number of individuals that will have their PII stored in this system: 200,000

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): 4/29/2011

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 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):

24VA19 and 79VA19

24VA19 – Patient Medical Records – VA and the legal authority is Title 38, United States Code, Sections 501(b) and 304.

79VA19 - Veterans Health Information Systems and Technology Architecture (VistA) Records-VA and the legal authority is: Title 38, United States Code, section 7301(a).

2. Name of the System of Records:

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

http://www.rms.oit.va.gov/SOR_Records.asp

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

Yes

Does the System of Records Notice require modification or updating?

No

(Please Select Yes/No)

Is PII collected by paper methods?

Yes

Is PII collected by verbal methods?

Yes

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

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)	ALL	This data will be used by management and for provision of healthcare, healthcare operations, billing of patient care episodes, mailing lists for research, provision of new services, recalls of medications, quality of assurance of health care activities, and public health surveillance. When data is collected for research project, the uses of data vary. Patients will be informed of all general uses of data. Where a specific risk will be encountered, the patient will be requested to sign an informed consent which notifies them in writing (in addition to the verbal summation) of known risks. The subject will be informed of all risks, uses, users, and whether or not he/she will benefit from the project.	All	All
Family Relation (spouse, children, parents, grandparents, etc)	Paper & Electronic	The data will be used primarily for research purposes. The subjects will be notified of all risks, uses, and users of the data. When used for health care operations, demographics of family are used for contacting in an alternate decision maker in the event the patient is incapacitated and rarely for infectious disease surveillance.	All	All

Service Information	ALL	<p>The individual will be notified that the data may be used to verify eligibility for care (or specific services) in the VA system. Occasionally a service record is important as part of the patient's medical history required for diagnosis. When this occurs, the patient will be told their service record is being reviewed. When used for research, the purpose of the research. Sometimes the Institutional review Board will approve waiver of informed consent. This is typically used with retrospective studies.</p>	All	All
Medical Information	ALL	<p>The patient is told in the VA's Notice of Privacy Practices that their information will be used for diagnosis and treatment, eligibility and enrollment, quality improvement, public health surveillance, abuse reporting, patient directories, as required by law, workers compensation cases, services, health care operations, training of medical students, oversight and accreditation and billing.</p>	All	All
Criminal Record Information	Electronic/File Transfer	<p>Patients are notified that information will be used as required by law and for criminal investigations and matters of National Security</p>	Written	Written
Guardian Information	ALL	<p>Patients are informed that this data is needed for research, funeral matters, billing, health care operations, abuse reporting, and social work support. When the data will be used for research in most cases, an informed consent will be obtained from the guardian, or the data will be collected under an Institutional Review Board waiver.</p>	All	All

Education Information	ALL	I collected for research, the individual will be told the specific reasons why this data will be requested. If the individual is a workforce member, the training is mandatory and they are notified of this in the process of taking the training.	Verbal & Automatic	Automated
Benefit Information	ALL	the patient is informed that the data is required for eligibility and enrollment.	All	All
Other (Explain)		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		

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	Veteran	Mandatory	Verbal or written informed consent
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	Verbal or written informed consent
Service Information	Yes	Veteran	Mandatory	Verbal or written informed consent
Medical Information	Yes	Veteran	Mandatory	Verbally, on the phone, automated, and paper.
Criminal Record Information	No			
Guardian Information	No			
Education Information	Yes	Veteran	Voluntary	Verbal or written informed consent

Benefit Information

No

Education Information for workforce
members

Yes

Other (Explain)

Mandatory

Verbally as part of
orientation

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	None				
Other Veteran Organization	None				
Other Federal Government Agency	None				
State Government Agency	None				
Local Government Agency	None				
Research Entity	None				
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system?	No
Please enter the name of the system:	
Per responses in Tab 4, does the system gather information from an individual?	No
If information is gathered from an individual, is the information provided:	<input type="checkbox"/> Through a Written Request <input type="checkbox"/> Submitted in Person <input type="checkbox"/> Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	Yes

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?	No
if yes, please check all that apply:	<input type="checkbox"/> Drug/Alcohol Counseling <input type="checkbox"/> Mental Health <input type="checkbox"/> HIV <input type="checkbox"/> Research <input type="checkbox"/> Sickle Cell <input type="checkbox"/> Other (Please Explain)
Describe process for authorizing access to this data.	
Answer:	

(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: Patient health information if disclosed could

Explain how collected data are limited to required elements:

Answer: Processes are in place to ensure collection of only required data. Data is collected and entered electronically with the use of automated forms that request only the data necessary. The use of these forms would then eliminate the collection of unnecessary data. Data collected by means of telephone are done so by completed paper forms that identify required data necessary. For example, an "Admission" form would be completed to admit a patient, therefore, only the data of these required fields would be collected.

How is data checked for completeness?

Answer: Data is reviewed by staff and confirmed and also compared to paper forms after data is entered electronically to ensure that all fields have been completed.

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

Answer: Administrative data is updated with each application for care. Each time a veteran is seen for an appointment, hospitalization, travel pay, etc. Data is verified and updated at the time the patient presents for care or follow-up. For example, clinics verify address, next of kin and insurance information.

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

Answer: New data is compared with printed form or via patient verification. The veteran brings 00214 with them and it is verified. For example, the 1010 is printed and the veteran reviews and signs that the information is accurate. For example, the VISTA system is designed to identify inconsistencies in data that is reported and provides an exception list for several applications

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

Answer: N/A

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: The retention period is dependent on the type of data and the intended use, so retention period varies. VA Records Control Schedule 10-1 (page 8): Records Management Responsibilities: The Health Information Resources Service (HIRS) is responsible for developing policies and procedures for effective and efficient records management throughout VHA. In addition, HIRS acts as the liaison between VHA and National Archives and Records Administration (NARA) on issues pertaining to records management practices and procedures. Field records officers are responsible for records management activities at their facilities. Program officials are responsible for creating, maintaining, protecting, and disposing of records in their program area in accordance with NARA regulations and VA policy. All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures. Local policy Medical Center Memorandum 590-136-19 "Records Management Policy".

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

Answer: Mandatory requirements are set for each type of data stored.

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.

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 using technical and managerial control mechanisms. Local Records Management Policy, Medical Center Memorandum 590-136-19 "Records Management Policy".

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

No

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: The system's security controls are certified every three years by an independent entity. The system owner, the Regional Information Officer reviews the recommendations and authorizes the system if appropriate. Plans of Action and Milestones are created and reviewed quarterly until closure. An annual risk assessment is conducted to detect changes in security controls and any newly identified vulnerabilities are added to the national database, Security Management And Reporting Tool. Plans of Actions and Milestones are created for these vulnerabilities. Also Information Technology Oversight and Compliance as well as the Office of the Inspector General review the system after the triennial Certification and Accreditation process is complete to validate the Plans of Actions and Milestones and the security controls that were certified as compliant.

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"/> Errors (Configuration and Data Entry) | <input checked="" type="checkbox"/> Storms/Hurricanes |
| <input checked="" type="checkbox"/> Communications Loss | <input checked="" type="checkbox"/> Fire (False Alarm, Major, and Minor) | <input checked="" type="checkbox"/> Substance Abuse |
| <input checked="" type="checkbox"/> Computer Intrusion | <input checked="" type="checkbox"/> Flooding/Water Damage | <input checked="" type="checkbox"/> Theft of Assets |
| <input checked="" type="checkbox"/> Computer Misuse | <input checked="" type="checkbox"/> Fraud/Embezzlement | <input checked="" type="checkbox"/> Theft of Data |
| <input checked="" type="checkbox"/> Data Destruction | | <input checked="" type="checkbox"/> Vandalism/Rioting |

Answer: (Other Risks)

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

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

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer: None, no choices were made regarding the project/system or collection of information as a result of performing the PIA.

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

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

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

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

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

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

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

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

Please add additional controls:

(FY 2011) PIA: Additional Comments

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



(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?

Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial	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 Performance 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 Entitlement Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Assistant	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	Telecare Record Manager	Web Automated Folder Processing System (WAFPS)
VBA Training Academy	VBA Enterprise Messaging System	Web Automated Reference Material System (WARMS)
Veterans Canteen Web	Veterans On-Line Applications (VONAPP)	Web Automated Verification of Enrollment
VIC	Veterans Service Network (VETSNET)	Web-Enabled Approval Management System (WEAMS)
VR&E Training Website	Web Electronic Lender Identification	Web Service Medical Records (WebSMR)
Web LGY		Work Study Management System (WSMS)

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

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

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

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

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?			
X ASISTS	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		ENDSOFT		RAFT
	A4P		Enterprise Terminology Server & VHA Enterprise Terminology Services		RALS
	Administrative Data Repository (ADR)		ePROMISE		Remedy Application
	ADT		EYECAP	X	SAN
	Agent Cashier		Financial and Accounting System (FAS)		Scanning Exam and Evaluation System
X	Air Fortress		Financial Management System	X	Sentillion
	Auto Instrument		Genesys		Stellant
	Automated Access Request	X	Health Summary Contingency	X	Stentor
	BDN 301		ICB		Tracking Continuing Education
	Bed Board Management System		KOWA		Traumatic Brain Injury
	Cardiff Teleform		Lynx Duress Alarm		VA Conference Room Registration VAMedSafe
	Cardiology Systems (stand alone servers from the network)		MHTP		
	CHECKPOINT	X	Microsoft Active Directory		VBA Data Warehouse
	Clinical Data Repository/Health Data Repository	X	Microsoft Exchange E-mail System		VHAHUNAPP1 VHAHUNFPC1
	Combat Veteran Outreach Committee on Waiver and Compromises		Military/Vet Eye Injury Registry Mumps AudioFAX		VISTA RAD Whiteboard
X	CP&E		NOAHLINK		
X	Crystal Reports Enterprise		Omnicell		
X	Data Innovations		Onvicord (VLOG)		
	DELIVEREX		Optifill		
	DICTATION-Power Scribe		P2000 ROBOT		
	DRM Plus		PACS database		
	DSIT		Personal Computer Generated Letters		
X	DSS Quadramed		PICIS OR		
	EDS Whiteboard (AVJED)	X	PIV Systems		
X	EKG System		Q-Matic		
	Embedded Fragment Registry		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
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?

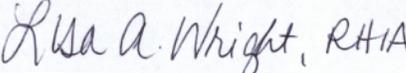
Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: Final Signatures

Facility Name: REGION 3 > VHA > VISN 06 > Hampton VAMC > LAN

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

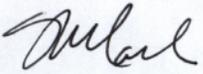
Privacy Officer:	Lisa Wright (Acting)	757-722-9961 x-1679	lisa.wright@va.gov
------------------	----------------------	---------------------	--------------------

	5/5/11
--	--------

Information Security Officer:	Timothy Brooks	757-722-9961 x-2584	timothy.brooks@va.gov
-------------------------------	----------------	---------------------	-----------------------

for 	5/5/2011
---	----------

System Owner/ Delegation of Authority	Kevin Marlowe	757-722-9961 x-2566	kevin.marlowe@va.gov
---------------------------------------	---------------	---------------------	----------------------

	5/5/11
--	--------

Network Information Security Officer:	Steven Blackwell	757-722-9961 x-7722	steven.blackwell@va.gov
---------------------------------------	------------------	---------------------	-------------------------

	5/5/2011
--	----------

Other Titles:	0	0	0
---------------	---	---	---

--	--	--	--

Date of Report: 5/5/11

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

Project Name REGION 3 > VHA > VISN 06 >

Hampton VAMC > LAN