(FY 2011) PIA: System Identification

Program or System Name:	Region 3>VHA.VISN 06>Durham VAMC>VistA		
OMB Unique System / Application / Program Identifier (AKA: UPID #):			OMB 300 ID 029-00-01-11-01-1180-00
Description of System/ Application/ Program:	This is the major application that houses most of the sensitive databases originating at the Durham VA Medical Center and it's outlying dependent entities. Databases may include but are not limited to the Computerized Patient Records System, Fiscal databases, Personnel databases, BAr Code Administration PAckage , Bed Management System, Emergency Department Information System, IMed for informed consent capture, etc.		
Facility Name:	Durham VA Medical Center		
Title:	**Name:**	**Phone:**	**Email:**
Privacy Officer:	Gregory Mavraganis	919-286-6991	Gregory.Mavraganis@va.gov
Information Security Officer:	Theresa Lynch	919-286-6839	Theresa.Lynch@va.gov
System Owner/ Chief Information Officer:	Toby Dickerson	919-286-6808	toby.dickerson@va.gov
Information Owner:	Ralph T. Gigliotti	919-286-6903	ralph.gigliotti@va.gov
Other Titles:			
Person Completing Document:	Theresa Lynch		
Other Titles:	Network Administrators and VistA System manager, Police Chief		
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)			07/2008
Date Approval To Operate Expires:			08/2011
What specific legal authorities authorize this program or system:			79 VA 19 Title 38, USC, 7301(a)
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.			25 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):	3/14/2011		

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?

- ☑ 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
2. Name of the System of Records:	Veterans Health Information Systems and Technology Architecture (VistA) Records-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/79VA19.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	The data will be used management and provision of healthcare, healthcare operations, billing of patient care episodes, mailing lists for research, provision of new services, recalls of medications, quality assurance of health care activities, public health surveillance. When data is collected for a research project the uses of the 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 an alternate decision maker in the event the patient is incapacitated and rarely for infectious disease surveillance.	All	All
Service Information	ALL	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 why their service record is being reviewed. When used for research, the purpose of the research. Sometimes the Institutional Review Board will approve a waiver of Informed Consent. This is typically used with retrospective studies.	All	All

Medical Information	ALL	The patient is told in the VA's Notice of Privacy Practices that their informatiom will be used for diagnosis and treatment, eligibility and enrollment, quality improvement, public health surveillance, abuse reporting, patient directories, as required by law, worker's compensation cases, services, health care operations, training of medical students, ovesight and accreditation and billing.	All	All
Criminal Record Information	Electronic/File Transfer	Patients are notified that information will be used as required by law and for criminal investigations and matters of national security	Written	Written
Guardian Information	ALL	Patients are informed that this data is needed for research, funeral matters, billing, health care operations, abuse reporting, social work support. When the data will be used for research in most cases, an informed consent will be ogtained from the guardian, or the data will be collected under an Institutional Review Board waiver.	All	All

Education Information	ALL	If 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)				

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	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	
Service Information	Yes	Veteran	Mandatory	
Medical Information	Yes	Veteran	Mandatory	Verbally, On the phone & automated
Criminal Record Information	No			

Guardian Information	Yes	Veteran	Voluntary	May also be supplied by family
Education Information	Yes	Veteran	Voluntary	Collected written, verbal, automated
Benefit Information	Yes	Veteran	Voluntary	Collected written, verbal, automated
Education Information for workforce members Other (Explain) Other (Explain)	Yes	Other (Explain)	Mandatory	Verbally as part of orientation.

(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	Falling Waters	Yes	All DATA	PHI	This is our storage area network (alternate processing site for VistA in case of disaster).
Other Veteran Organization	Other VISN 6 VA's	Yes	CPRS treatment and billing	Both PII & PHI	VistA Web, CAPRI and Remote access (SFTP)
Other Federal Government Agency					
State Government Agency					
Local Government Agency					
Research Entity	Multiple VAMC's	Yes	CPRS for Research	Both PII & PHI	VA Handbook 6500 and MCM 00.5
University Affiliate	Duke University	Yes	Medical data for patient treatment purposes and research.	PHI	There is a Citrix connection w/ the university that allows access to the medical record through remote procedure calls. There is a separate access agreement for this application that must be signed by the Service Chief and granted by an Information Security officer.
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

5. 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? 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: If the data is for research purposes there are several avenues for approval to use this data depending on the research project: written informed consent; waiver of documentation of informed consent, HIPAA waiver, verbal via telephone. All of these modalities must be approved by the Institutional Review Board and sometimes Research & Development Committee. If the use is for Quality improvement or health care operations, uses as required by law, etc. access is obtained via written request for access to the VA computer system, signed by a senior member of the Service, reviewed by the Information Security Officer and approved by Office of Information and Technology Staff. Information Security, Privacy and Compliance training must be complete prior to granting access. Access from Duke requires a separate agreement that must be signed by the Associate Medical Center Director, Service Chief (or designee) and Information Security Officer.

(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: Loss of PHI could be embarassing for the department as well as incur credit monitoring charges for each affected patient

Explain how collected data are limited to required elements:

Answer: System programming. The system is programmed with templates that limit answers to the type of information required. In some instances specific fields are limited to numbers, others may be limited to a choice of specific text responses. Still others may be free text.

How is data checked for completeness?

Answer: The Medical Records Committee monitors the content of the Medical Record. There is a contractor that also monitors select samples of records to ensure that Medical Center policies and procedures are followed regarding quality of care including electronic documentation. There are electronic measures such as check sum to verify integrity of the data. There are also alerts built into the VistA Lab package that notify the tech of abnormal values. Data is verified by a tech who must review the results.

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

Answer:All entries to records in VistA are time stamped and appear in chronolgical order by category within the Medical Record.

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

Answer: New entries in the Medical Record must be signed by the individual responsible for generating the data. Lab results are verified by the technologist performing the test. Radiology results are verified by a radiologist. Any entry made by a resident must be cosigned by an Attending Physician. Patient's demographic and financial data is required by policy to be reviewed upon appointment check in. Employee financial data can be reviewed at any time by the employee through Human Resources, Fiscal Service, MyPay.

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: Currently Research has no specific retention period listed VA Directive 6371, VA Directive 6300, VA HAndbook 6300.1, National Archives and Records Administration CFR and VA's RCS 10-1 and RCS 005.1. All other collected data follow NARA requirements and Records Control Schedule 10-1 and Office of Information & Technology (OI&T) Records Control Schedule (RCS) 005-1. Retention varies based on information type and usage.

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

Answer: Information is needed for Research, quality improvement,and medical center operations, audits by the OIG and JCAH, etc..

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

Answer: Paper materials are shredded at the end of retentiion period in accordance with VA Handbook 6300.1. Hard drives and other storage tapes are destroyed at end of life by over-write, degaussing and/or shredding. If data removal is required prior to end of life, specific files maybe overwritten. Electronic files are deleted when no longer needed.

Where are these procedures documented?

Answer: The Supervisor of the OI&T desktop support unit keeps records of destruction of har drives on a network share available to the ISOs for audit. The Chief Environmental management Service keeps records of destruction of paper and plastics. Currently all electronic records requiring protection cannot be destroyed.

How are data retention procedures enforced?

Answer: Environment of Care rounds reviews disposal of paper and look for cpu's that have been disconnected and are no longer in use. Inventory of computers is conducted every 6 months. Computers are assigned to a specific room. Port security is in place so that OI&T gets an immediate notification when someone tries to plug in a different computer. The Records Control Officer conducts training with records liasions to ensure that records are appropriately maintained. The Records Control Officer must review and approve all records listed on the Records Control Schedule prior to destruction. Destruction of hard drives has taken place on site and was overseen by Office of Information and Technology staff. Paper is shredded on site by a contractor and overseen by Environmental Management Staff. A certificate of destruction is issued immediately. Plastic media is sent off site for destruction by a contractor who must supply a certificate of destruction per contract. The Records Control Officer reviews file management practices including destruction at least annually.

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: research records are maintained indefinitely because no guidance has been issued on retention time.

(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? No

If 'No' please describe why:

Answer: The computer room, which houses the majority of servers and infrastructure is secured in accordance with VA Directive and Handbook 6500.

Some data closets in the facility and at CBOCs in Greeneville and Morehead City do not meet VA's physical security standards in that there is no electronic accesss control card, some walls do not go to the true ceiling, some closets do not have temperature controls or adequate space, some doors are not adequate and some unauthorized staff can gain access to these closets. This has been brought to the attention of the FAcility Director and is recorded as a POAM in Smart. The Facility Director has accepted risk until there is money and space available to bring the closets into compliance.

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 trienniel 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)*

- ☑ Air Conditioning Failure
- ☑ Chemical/Biological Contamination
- ☑ Blackmail
- ☑ Bomb Threats
- ☑ Data Disclosure
- ☑ Data Integrity Loss
- ☑ Denial of Service Attacks
- ☑ Earthquakes
- ☑ Hardware Failure
- ☑ Identity Theft
- ☑ Malicious Code
- ☑ Power Loss

- [x] Bomb Threats
- [x] Burglary/Break In/Robbery
- [x] Cold/Frost/Snow
- [x] Communications Loss
- [x] Computer Intrusion
- [x] Computer Misuse
- [ ] Data Destruction
- [x] Denial of Service Attacks
- [x] Earthquakes
- [x] Eavesdropping/Interception
- [x] Errors (Configuration and Data Entry)
- [x] Fire (False Alarm, Major, and Minor)
- [x] Flooding/Water Damage
- [x] Fraud/Embezzlement
- [x] Power Loss
- [x] Sabotage/Terrorism
- [x] Storms/Hurricanes
- [x] Substance Abuse
- [x] Theft of Assets
- [x] Theft of Data
- [x] Vandalism/Rioting

Answer: (Other Risks) Nuclear Terrorism

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: Port security, Sanctuary, Cisco Wireless security

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.
Answer: implemented port security to ensure no non-VA devices could be attached directly to the network. Implemented Sanctuary to ensure that personal portable devices that connect via USB cable are blocked to prevent removal of sensitive information. Use Sanctury to block the unauthorized downloading of sensitive information to a cd. Instituted visibility to the desk top and SCCM to automate patching and make it eaasier to identify universal vulnerabilities.

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 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.

individuals what will the potential impact be upon the system or organization? **(Choose One)**

- [illegible] 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 th

There were many applications that reside on the network and VistA but were left off

System	Name of Application	Description	Collects	Stores
VistA	Audiology	TBI testing	PHI	PHI
VistA	DSIT	Telecare Records Manager	PHI	PHI
VistA	DSS QuadraMed	Coding/Billing	PHI	yes
VistA	EDIS Whiteboard	Status boards	PII	PII
VistA	Eye View	Images of the elements of the e	PHI	PHI
VistA	Imed Consent	Electronic informed Consent	PHI	PHI
VistA	MUSE	EKG	PHI	PHI
VistA	Natus EEG	Record sleep study EEG's	PHI	PHI
VistA	Omnicell	Drug Dispensing	PHI	PHI
VistA	Pilcam Software	Camera colonoscopies	PHI	PHI
VistA	Rural Health	Recruitment and treatment of V	PHI	PHI
VistA	Script Pro	Drug dispensing	PHI	PHI
VistA	Telecare Records Manager	Remote Home Healthcare	PHI	PHI
VistA	Traumatic Brain Injury	OEF/OIF	PHI	PHI
VistA	Veterans Identity Card (VIC)	Patient Identification	PII	PII
VistA	Xcelera	Cardiac imaging	PHI	PHI

e question you are responding to and then add your comments.

one list or another. They are listed below

Accessed by:	Storage Location
Audiology staff	VistA Cluster
Telehealth staf	VistA Cluster
Billing staff & C	Storage Area network
Nursing + Adm	Storage Area network
Opthmalogy S	VistA Imaging
Clinical staff	Vista Cluster
EEG staff	VistA Cluster
EEG Technicia	Natus
Pharmacists	VistA Cluster
Clinicians & pa	VistA Cluster
Rural Health St	Vista Cluster
Pharmacists	Script pro
Nursing + Adm	VistA Cluster
Social Workers	VistA Cluster
Administrative :	Storage Area network
Cardiology staf	VistA Imaging

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?

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 Asisstant
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 Bar Code Med Admin	x Auto Replenishment/ Ward Stock
X CMOP	x Clinical Reminders	x Clinical Case Registries	x Automated Info Collection Sys
X Dental Imagi	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 Data base	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 Vertified 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
	Administrative Data Repository (ADR)		ePROMISE		Remedy Application
	ADT		EYECAP		SAN
	Agent Cashier		Financial and Accounting System (FAS)		Scanning Exam and Evaluation System
X	Air Fortress	X	Financial Management System	X	Sentillion
	Auto Instrument		Genesys		Stellant
	Automated Access Request	X	Health Summary Contingency	X	Stentor
	BDN 301	X	ICB		Tracking Continuing Education
X	Bed Board Management System		KOWA		Traumatic Brain Injury
	Cardiff Teleform		Lynx Duress Alarm		VA Conference Room Registration
	Cardiology Systems (stand alone servers from the network)		MHTP		VAMedSafe
	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		Military/Vet Eye Injury Registry		VHAHUNFPC1
	Committee on Waiver and Compromises	X	Mumps AudioFAX	X	VISTA RAD
X	CP&E	X	NOAHLINK		Whiteboard
X	Crystal Reports Enterprise	X	Omnicell		
X	Data Innovations		Onvicord (VLOG)		
	DELIVEREX		Optifill		

	DICTATION-Power Scribe		P2000 ROBOT
X	DRM Plus	X	PACS database
X	DSIT	X	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

(FY 2011) PIA: Final Signatures

Facility Name:	Region 3>VHA.VISN 06>Durham VAMC>VistA		
Title:	Name:	Phone:	Email:
Privacy Officer:	Gregory Mavraganis	919-286-6991	Gregory.Mavraganis@va.gov
Information Security Officer:	Theresa Lynch	919-286-6839	Theresa.Lynch@va.gov
Theresa G. Lynch	Digitally signed by Theresa G. Lynch DN: c=US, o=U.S. Government, ou=Department of Veterans Affairs, ou=Internal Staff, 0.9.2342.19200300.100.1.1=Theresa.Lynch@va.gov, cn=Theresa G. Lynch Date: 2011.03.22 13:29:01 -04'00'		
System Owner/ Chief Information Officer:	Toby Dickerson	919-286-6808	toby.dickerson@va.gov
Information Owner:	Ralph T. Gigliotti	919-286-6903	ralph.gigliotti@va.gov
Other Titles:	0	0	0
Digital Signature Block			
Date of Report:	3/14/11		
OMB Unique Project Identifier	OMB 300 ID 029-00-01-11-01-1180-00		
Project Name	Region 3>VHA.VISN 06>Durham VAMC>VistA		