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://vaww.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 indentify 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 to received full credit for submission.

(FY 2011) PIA: System Identification

Program or System Name:	REGION 3 > VHA > VISN 10 > Columbus VA ACC > LAN
OMB Unique System / Application / Program Identifier (AKA: UPID #):	029-00-02-00-01-1120-00
Description of System/ Application/ Program:	The Local Area Network (LAN) system is comprised of workstations, servers, printers and other equipment which include devices such as routers, hubs, switches, and firewalls that support communications to extended LAN locations such as community based outpatient clinics (CBOCs).

Facility Name: Chalmers P. Wylie VA Ambulatory Care Center

Title:	Name:	Phone:	Email:
Privacy Officer:	Shelley Leister	614-257-5626	shelley.leister@va.gov
Information Security Officer:	Shaunna J. Ford	614-257-5981	Shaunna.Ford@va.gov
System Owner/ Chief Information Officer:	Chris Baxter	614-388-7000	Chris.Baxter@va.gov
Information Owner:	Lay, Michael R3 Director		Michael.Lay@va.gov
Other Titles:			
Person Completing Document:	Shaunna J. Ford	614-257-5981	Shaunna.Ford@va.gov
Other Titles:	Dave Fultz, Network Admin	614-257-5485	Dave.Fultz@va.gov

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	04/2010 Validation Letter
Date Approval To Operate Expires:	08/2011
What specific legal authorities authorize this program or system:	Title 38, U.S.C, section 7301(a), Functions of Veterans He
What is the expected number of individuals that will have their PII stored in this system:	1-250,000
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.	13 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):	04/2011

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

- ☑ Have any changes been made to the system since the last PIA?
- ☑ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- ☑ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- ☑ Does this system/application/program collect, store or disseminate PII/PHI data?
- ☑ Does this system/application/program collect, store or disseminate the SSN?

☑ Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please complete TAB 7 & TAB 12. (See Comment for Definition of PII)

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.	Yes
For each applicable System(s) of Records, list:	
1. All System of Record Identifier(s) (number):	79VA19 24VA19
2. Name of the System of Records:	Patient Medical Records-VA and *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://vaww.vhaco.va.gov/privacy/SystemofRecords.htm
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?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	ALL	How it will be used, managed and shared	All
Family Relation (spouse, children, parents, grandparents, etc)	ALL	How it will be used, managed and shared	All
Service Information	ALL	How it will be used, managed and shared	All
Medical Information	ALL	How it will be used, managed and shared	All
Criminal Record Information	ALL	How it will be used, managed and shared	All
Guardian Information	ALL	How it will be used, managed and shared	All
Education Information	ALL	How it will be used, managed and shared	All
Benefit Information	ALL	How it will be used, managed and shared	All
Other (Explain)	N/A	How it will be used, managed and shared	All

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?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Other (Explain)	Mandatory
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Other (Explain)	Mandatory
Service Information	Yes	Other (Explain)	Mandatory
Medical Information	Yes	Other (Explain)	Mandatory
Criminal Record Information	Yes	Other (Explain)	Mandatory
Guardian Information	Yes	Other (Explain)	Mandatory
Education Information	Yes	Other (Explain)	Mandatory
Benefit Information	Yes	Other (Explain)	Mandatory
Other (Explain)			
Other (Explain)			
Other (Explain)			

How is a privacy notice provided?

All

All

All

All

All

All

All

All

All

Additional Comments

The Source of information varies as it relates to the need. For instance, Emergency Call back lists are created by Program Managers in order to comply with Emergency Operations activities

Varies, these could be extracts from Vista or directly from the patient (such as the creation of a spreadsheet for tracking patients in surgery who have NOK or Family with them.)

Comes from multiple sources, VBA, Directly from individuals, etc.

Sources vary

Sources vary

Sources vary

Sources vary

Sources vary

(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?
Internal Sharing: VA Organization	Contracting; VBA; VCS; OI&T; Field Security Service	Yes	Payroll, Benefits, PII/PHI, Background Investigations	Both PII & PHI
Other Veteran Organization	Veterans Service Office (e.g. DAV, Marine Corp League, etc.)	Yes	Connects to LAN in order to access VBA.	N/A
Other Federal Government Agency	Regional Counsel	No	Medical/Admin/Legal	Both PII & PHI
State Government Agency	Depart of Health	No	Medical/Public Safety	PHI
Local Government Agency	County Coroner	No	Medical/Certificates of Death	Both PII & PHI
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?

Please enter the name of the system: Vista-VMS (Not automatically - Reports may be extracted

Per responses in Tab 4, does the system gather information from an individual?

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?

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?

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: Research is in accordance with VHA Directive 1200 and associated publications. Protocols are reviewed by PO and ISC on by IRB and R&D of record. All others are by patient authorization or routine use in related SOR.

What is the procedure you reference for the release of information?

VA Directive 6502, Enterprise Privacy; Privacy Act of 1974, 38 USC 5701, 38 USC 7332, 5 USC 552 FOIA, 38 USC 5705, HIPAA Privacy Rule

VA Directive 6502, Enterprise Privacy; Privacy Act of 1974, 38 USC 5701, 38 USC 7332, 5 USC 552 FOIA, 38 USC 5705, HIPAA Privacy Rule

Only when required in accordance with VA Privacy Policy

Privacy Policy

Privacy Policy

Yes

by end users)

Yes

Yes

) then reviewed and voted

(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 validation for electronic and by use of templates and policy requirements

How is data checked for completeness?

Answer: Data Validation, manually and through audits

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

Answer: Pre-registration at time of visit, Mandatory Patches

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

Answer: Self reporting, HINQ, Insurance 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: Retention is in accordance with NARA regulations and VA Policy, VA Records Control Schedule based on the recordsPaper records and information stored on electronic storage media are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States, and VA policies and procedures for media sanitization, e.g., RCS 10-1. Longest retention period is 75 yrs for medical records.

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

Answer: To comply with Federal Laws; Ongoing Patient Care, Research

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

Answer:All VHA employees are responsible for ensuring that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures. For Electronic media that meets the disposal criteria based on the category of data, the media will be destroyed in accordance with NIST 800-88 and Media Sanitization Policies.

Where are these procedures documented?

Answer: VA Directives 6300, 6300.1, VHA RCS 10-1; VA Handbook 6500 and related 6500.1, and 6500 Appendix D.

How are data retention procedures enforced?

Answer: Field records officers are responsible for records management activities at their facilities.

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? No

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? No

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? No

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

Answer: The requirements for Continuous Monitoring are yearly when not in a Certification and Accreditation year which is every three years or when there is a significant change. Columbus VA ACC underwent SCA Testing 5/2010

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: As a General Support System with a High System Categorization, requirements for SCA Testing in accordance with Federal laws and regulations are in place.

Explain what security risks were identified in the security assessment? *(Check all that apply)*

- ☑ Air Conditioning Failure
- ☑ Chemical/Biological Contamination
- ☑ Blackmail
- ☑ Bomb Threats
- ☑ Burglary/Break In/Robbery
- ☑ Cold/Frost/Snow
- ☑ Communications Loss
- ☑ Computer Intrusion
- ☑ Computer Misuse
- ☑ Data Destruction
- ☑ Data Disclosure
- ☑ Data Integrity Loss
- ☑ Denial of Service Attacks
- ☑ Earthquakes
- ☑ Eavesdropping/Interception
- ☑ Errors (Configuration and Data Entry)
- ☑ Fire (False Alarm, Major, and Minor)
- ☑ Flooding/Water Damage
- ☑ Fraud/Embezzlement
- ☑ Hardware Failure
- ☑ Identity Theft
- ☑ Malicious Code
- ☑ Power Loss
- ☑ Sabotage/Terrorism
- ☑ Storms/Hurricanes
- ☑ Substance Abuse
- ☑ Theft of Assets
- ☑ Theft of Data
- ☑ Vandalism/Rioting

Answer: (Other Risks)

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

- ☑ 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) Privacy Controls in accordance with NIST 800-53 Rev. 3

PIA: PIA Assessment

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

Answer: Additional training and awareness in order to mitigate mishandling of VA SPI. In a survey of staff on the use or generating of VA SPI, a small percentage were found saving information in an unsecure manner. This data has been moved to secure storage and education provided to those users. Biomedical equipment requires vigilance in applying the security controls above in order to protect and maintain the data.

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]
- 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.

Tab 5 Row 35: Under Other, State Department of Health, BMV

Tabs 3, 4 and 6: PII may be stored on the LAN, but the LAN does not collect PII for it's purposes. PII that is stored on the LAN are from extracts for use for reporting of aggregate data, follow up of consults, tracking of service specific issues, etc.

Other PII stored on the LAN within databases created and used by biomedical devices may or may not be stored within Vista which would be covered by the SOR for Patient Medical Record or VISTA, however, would be data covered under the appropriate SOR.

These biomedical devices have security controls applied to them accordingly and the corresponding databases have access controls, identification and authentication controls applied to ensure limited access. These electronic files are protected in accordance with all other data retention methods mentioned in previous tabs.

Tab 11: Many of the Minor applications mentioned in this TAB are GUI to Vista. The data itself for these minor apps are not stored directly on the LAN but within VISTA.

Tab 11: Additional Minor Apps: The following are devices from the Medical Device Protection Program that collect PII:

(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?

ASISTS
Bed Control
CAPRI
CMOP
Dental
Dietetics
Fee Basis
GRECC
HINQ
IFCAP
Imaging
Kernal
Kids
Lab Service
Letterman
Library
Mailman
Medicine
MICOM
NDBI
NOIS
Oncology
PAID
Prosthetics
QUASER
RPC Broker
SAGG
Scheduling
Social Work
Surgery
Toolkit
Unwinder
VA Fileman
VBECS
VDEF
VistALink

Beneficiary Travel
Care Management
Care Tracker
Clinical Reminders
CPT/ HCPCS Codes
DRG Grouper
DSS Extracts
Education Tracking
Engineering
Event Capture
Extensible Editor
Health Summary
Incident Reporting
Intake/ Output
Integrated Billing
Lexicon Utility
List Manager
Mental Health
MyHealthEVet
National Drug File
Nursing Service
Occurrence Screen
Patch Module
Patient Feedback
Police & Security
Problem List
Progress Notes
Record Tracking
Registration
Run Time Library
Survey Generator
Utilization Review
Visit Tracking
VistALink Security
Women's Health

Accounts Receivable
ADP Planning (PlanMan)
Bad Code Med Admin
Clinical Case Registries
Clinical Procedures
Consult/ Request Tracking
Controlled Substances
Credentials Tracking
Discharge Summary
Drug Accountability
EEO Complaint Tracking
Electronic Signature
Event Driven Reporting
External Peer Review
Functional Independence
Gen. Med. Rec. - I/O
Gen. Med. Rec. - Vitals
Generic Code Sheet
Health Level Seven
Hospital Based Home Care
Inpatient Medications
Integrated Patient Funds
MCCR National Database
Minimal Patient Dataset
National Laboratory Test
Network Health Exchange
Outpatient Pharmacy
Patient Data Exchange
Patient Representative
PCE Patient/ HIS Subset
Security Suite Utility Pack
Shift Change Handoff Tool
Spinal Cord Dysfunction
Text Integration Utilities
VHS & RA Tracking System
Voluntary Timekeeping

Adverse Reaction Tracking
Authorization/ Subscription
Auto Replenishment/ Ward Stock
Automated Info Collection Sys
Automated Lab Instruments
Automated Med Info Exchange
Capacity Management - RUM
Capacity Management Tools
Clinical Info Resource Network
Clinical Monitoring System
Enrollment Application System
Equipment/ Turn-in Request
Gen. Med.Rec. - Generator
Health Data and Informatics
ICR - Immunology Case Registry
Income Verification Match
Incomplete Records Tracking
Interim Mangement Support
Master Patient Index VistA
Missing Patient Reg (Original) A4EL
Order Entry/ Results Reporting
PCE Patient Care Encounter
Pharmacy Benefits Mangement
Pharmacy Data Management
Pharmacy National Database
Pharmacy Prescription Practice
Quality Assurance Integration
Quality Improvement Checklist
Radiology/ Nuclear Medicine
Release of Information - DSSI
Remote Order/ Entry System
Utility Management Rollup
CA Vertified Components - DSSI
Vendor - Document Storage Sys
Visual Impairment Service Team ANRV
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?

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

(FY 2011) PIA: Final Signatures

Facility Name: REGION 3 > VHA > VISN 10 > Columbus VA ACC > LAN

Title:	Name:	Phone:	Email:
Privacy Officer:	Shelley Leister	614-257-5626	shelley.leister@va.gov
5/4/2011			
X Shelley A. Leister			
Privacy Officer			
Information Security Officer:	Shaunna J. Ford	614-257-5981	Shaunna.Ford@va.gov
5/4/2011			
X Shaunna J. Ford			
Information Security Officer			
System Owner/ Chief Information Officer:	Chris Baxter	614-388-7000	Chris.Baxter@va.gov
5/4/2011			
X Chris Baxter			
Facility Chief Information Officer			
Information Owner:	Lay, Michael R3 Director		0 Michael.Lay@va.gov

Other Titles:	Chris Baxter	614-388-7000	Chris.Baxter@va.gov

Digital Signature Block

Date of Report:	4/1/11
OMB Unique Project Identifier	029-00-02-00-01-1120-00
Project Name	REGION 3 > VHA > VISN 10 > Columbus VA ACC > LAN