

Welcome to the PIA for FY 2011!

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

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

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

Directions:

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

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

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

Roles and Responsibilities:

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

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

Definition of PII (Personally Identifiable Information)

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

Macros Must Be Enabled on This Form

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

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

All Macros; 2) Click OK

Final Signatures

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

Privacy Impact Assessment Uploaded into SMART

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 > Vista-VMS
 OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-01-11-01-1180-00

Description of System/ Application/ Program: A customizable relational database containing applications and data for clinical and administrative functions in use at the VA ACC, Columbus.

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 Ford	614-257-5981	Shaunna.ford@va.gov
System Owner/ Chief Information Officer:	Lay, Michael R3 IS Director		Michael.Lay@va.gov
Information Owner:			
Other Titles:	Chris Baxter, FCIO	614-388-7000	Chris.baxter@va.gov
Person Completing Document:	Shelley Leister	614-257-5626	shelley.leister@va.gov
	Bryan Lucas, Vista Systems		
Other Titles:	Manager	514-257-5480	Bryan.Lucas@va.gov
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)			7/1/2008 (Validation Letter 4/2010)
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 Health Administration

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. 2/15/2008 Moved system to new facility location November 2010

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): 02/2011

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

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

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

(FY 2011) PIA: System of Records

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

Yes

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

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

79VA19

2. Name of the System of Records:

Veterans Health Information System and Technology
Architecture - Vista

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?

No

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)	Paper & Electronic	Used for the purpose of Healthcare Benefits, Eligibility, Contact, etc.	Verbal & Automatic	Written
Family Relation (spouse, children, parents, grandparents, etc)	Paper & Electronic	Next of Kin, DNR instructions, HealthCare Proxy Designations, Eligibility (based on income).	Verbal & Automatic	Written
Service Information	ALL	Collected to determine eligibility status and service connection designation (if any).	All	Written
Medical Information	ALL	Used to determine medical history, diagnosis and treatment of the patient	Verbal & Written	Written
Criminal Record Information	Electronic/File Transfer	Used in conjunction with the Fugitive Felon Program, in compliance with the Fugitive Felon portion of PL 107-103 § 505	Verbally	Written
Guardian Information	Paper & Electronic	Next of Kin, DNR instructions, health care proxy designation.	Verbal & Written	Written
Education Information	Paper	Used for credentialing for Employees WOC - Students)	Verbal & Written	Written
Benefit Information	Paper & Electronic	Medical benefits they maybe eligible for may be based on other VA benefits, e.g. service-connection, non-service connection pensions, Aid & Attendance, etc.	Verbal & Written	Written
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	
Service Information	Yes	Other (Explain)	Mandatory	Source of data may come from the veteran (with or without DD214) Additionally verificatio of service may be obtained through request process known as Hospital Inquiry through VBA
Medical Information	Yes	Other (Explain)	Voluntary	
Criminal Record Information	Yes	Other (Explain)	Mandatory	OIG, Police (local, County, State, Federal)

Guardian Information	Yes	Other (Explain)	Mandatory	This information can come from multiple sources, e.g., local courts, attorneys, veteran, et. al.
Education Information	Yes	Other (Explain)	Voluntary	For Veterans this information is voluntary, however, from VA staff it is mandatory
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	VBA-provided data for verification of service, service-connection, Non-Service connected pensions, etc.
Other (Explain)				
Other (Explain)				
Other (Explain)				

(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VBA; Readjustment Counseling; Regional Council; Austin Automation Center; Centralized Mail Out Pharmacy; National Prosthetic Patient Database, eCMD	Yes	VBA/Regional Office: treatment and demographic for benefits determination. Regional Council: Tort Claims, legal processes. BAA in place. AAC - Workload, Fiscal, Claims; DDC - In conjunction with Prosthetics for issuance of certain Prosthetic items, eg. hearing aids; pressure socks, etc.; CMOP - RX and demographic information mailed out to patients; NPPD - Treatment, Benefits, Administrative	Both PII & PHI	1605.1
Other Veteran Organization	Veteran Service, e.g. Military Order of the Purple Heart; Disabled American Veterans; Veterans of Foreign Wars, etc.	Yes	Medical records relating to claims processing on behalf of the veterans	Both PII & PHI	1605.1 and Power of Attorney

Other Federal Government Agency	FBI; OPM; DEA; DOD; Centers for Disease Control; Social Security Administration; Internal Revenue; various Congress or Senators depending on district of the constituent	Yes	Congressional inquiries accompanied by patient authorization; various information including appointment dates, treatment, medical documentation; billing; co-pay. In addition, certain clinical data is shared with CDC.	Both PII & PHI	VA Handbook 1605.1
State Government Agency	State Police; Ohio BMV; Department of Health; Ohio Department of Job and Family Services	No	As they pertain to standing letters.	Both PII & PHI	VA Handbook 1605.1
Local Government Agency	Local Police; County Coroner	No	Medical data to assist in the completion of death certificates	Both PII & PHI	VA Handbook 1605.1
Research Entity	VAMC-Cincinnati with MOU with University of Cincinnati Medical School	No	Hard Copy research information such as, consents, research protocols, etc. The purpose is to approve and monitor research studies.	Both PII & PHI	VA Handbook 1605.1 and VHA 1200.05

Other Project / System
Other Project / System
Other Project / System

(FY 2011) PIA: Access to Records

Does the system gather information from another system? Yes
Please enter the name of the system: DOD and Tri_Care and Austin Automation; Health Eligibility Center (CBO)
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: 1. D/A , HIV, Sickle Cell records/counseling require informed consent authorization mentioning this specific type of data signed by the patient/legal representative . 2.MH data would require a patient/legal representative signed authorization. All could be subject to Routine Uses in SOR 24VA19. Research data requires consents and authorizations and also may involve de-identification, coding or disclosing as aggregate data.

(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: Standardized VA forms, Limitations within Vista Applications, Access Limitations (Minimum Necessary/Functional Category)of users.

How is data checked for completeness?

Answer: Manually as well as input validation within the Vista software to ensure data integrity

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

Answer: Policy Memo updates; Standard Operating Procedures and VA Directives;HEC Notifications

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

Answer: Manually and through automatic means through Austin when data is rejected. In addition identification and authentication controls are in place within Vista ensuring that each process is coupled with a unique identifier for auditability and assurances that data is traceable.

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: Dependent on the SOR, but the longest is the Patient Medical Record which is 75 Years after the last episode of Patient Care

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

Answer: Clinical Information is retained in accordance with VA Records Control Schedule 10-1. Demographic information is updated as applications for care are submitted and retained in accordance with RCS 10-1.

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

Answer: Records in electronic format that meet destruction criteria based on RCS10-1 are "sanitized" using NIST SP800-88 and VA Handbook 6500.1 Media Sanitization processes and procedures. Hardcopy/paper data are destroyed per timeframes in RCS-10 and current privacy/security methods, e.g., incineration, pulverizing.

Where are these procedures documented?

Answer: VA Handbook 6500.1 Media Sanitization & VA Directive 6371, Destruction of Temporary Paper Records

How are data retention procedures enforced?

6. Program LVL Questions

Answer: Records Management Program Media Protection Policies

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: Security Categorization in accordance with FIPS 199 indicates that Vista-VMS has a security categorization of High. FIPS 200 dictates the "minimum security requirements for Federal Information Systems. Therefore, NIST 800-53 determines the controls that are to be applied to high systems.

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 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 type="checkbox"/> Substance Abuse |
| <input checked="" type="checkbox"/> Computer Intrusion | <input checked="" type="checkbox"/> Fire (False Alarm, Major, and Minor) | <input checked="" type="checkbox"/> Theft of Assets |

Computer Intrusion

Computer Misuse

Data Destruction

Fire (False Alarm, Major, and Minor)

Flooding/Water Damage

Fraud/Embezzlement

Theft of Assets

Theft of Data

Vandalism/Rioting

Answer: (Other Risks) Dust/Debris; Humidity

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

PIA: PIA Assessment

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

Answer: Currently there are no changes needed in the collection source or methods. Controls are selected exclusively for the project/system or inherited by the General Support System in order to mitigate any risks.

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

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

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

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

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

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

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

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

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

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

(FY 2011) PIA: Final Signatures

Facility Name: Region 3 > VHA > VISN 10 > Columbus VA ACC > Vista-VMS

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

Privacy Officer:	Shelley Leister	614-257-5626	shelley.leister@va.gov
------------------	-----------------	--------------	------------------------

4/20/2011

X

Shelley A. Leister

Shelley Leister

Information Security Officer:	Shaunna Ford	614-257-5981	Shaunna.ford@va.gov
-------------------------------	--------------	--------------	---------------------

4/20/2011

X

Shaunna J. Ford

Shaunna J. Ford

System Owner/ Chief Information Officer:	Lay, Michael R3 IS Director	614-257-5981	Michael.Lay@va.gov
--	-----------------------------	--------------	--------------------

Information Owner:	Lilian T. Thome, MD	614-257-5450	Lilian.Thome@va.gov
--------------------	---------------------	--------------	---------------------

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

4/20/2011

X Chris Baxter

Chris Baxter

Facility Chief Information Officer

OMB Unique Project Identifier

Project Name

2/1/11

029-00-01-11-01-1180-00

Region 3 > VHA > VISN 10 >

Columbus VA ACC > Vista-VMS