

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 4>VHA>VISN 04>Wilmington VAMC>LAN
 OMB Unique System / Application / Program Identifier (AKA: UPID #):
 The LAN system is the hardware infrastructure on which this facility supports Government initiatives, also known as, General Support System (GSS) such as routers, switches, printers, workstations, servers, and wireless services across the Wilmington VA Medical Center (VAMC), and the facility in Dover DE, Georgetown DE, Cape May NJ, Ventnor NJ and Vineland NJ supports the delivery of healthcare to veterans. The LAN support: application for Wilmington VAMC, housing all patient health information.

Description of System/ Application/ Program: application for Wilmington VAMC, housing all patient health information.

Facility Name: Wilmington VAMC

Title:	Name:	Phone:
Privacy Officer:	Miguel Sanchez	(302) 994-2511 x4750
Information Security Officer:	Mary K. Jones	(302) 633-5551
System Owner/ Chief Information Officer:	Jack Galvin/Scott Viars	(518) 626-6244/(302) 644-5450
Information Owner:	Charles M. Dorman	(302) 633-5201
Other Titles:		

Person Completing Document: Mary K. Jones
 Other Titles:
 Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)
 Date Approval To Operate Expires:

What specific legal authorities authorize this program or system:
 What is the expected number of individuals that will have their PII stored in this system:
 Identify what stage the System / Application / Program is at:
 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.

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

If No, please explain:

Has a PIA been completed within the last three years?

Date of Report (MM/YYYY):

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 7 & TAB 12. (See Commen

029-00-02-00-01-1120-00

ty operates its software applications and support for E-
3SS). It includes the computer hardware and equipment
3less. The Wilmington VAMC LAN system supports IT
3e Community Based Outpatient Clinics (CBOCS) located
and NJ. The LAN provides critical connectivity that
3s the VistA major application which is the patient care
3rmation and eligibility data for VA patients. Personal

Email:

miguel.sanchez@va.gov

mary.jones3@va.gov

scott.viars@va.gov

charles.dorman@va.gov

11/2009

08/2011

Title 38, United States Code, Sections 501(b) and 304

126972

Operations/Maintenance

In operation since 1998.

Yes

Yes

01/2011

orm.

contractors, or others performing work for
unique identifier, symbol, or other

2. System Identification

unique identifier, symbol, or other

(it for Definition of PII)

(FY 2011) PIA: System of Records

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

Yes

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

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

24VA19

2. Name of the System of Records:

Patient Medical 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?

No

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)	VA File Database	The LAN system shares information with VistA and VistA resides on the LAN. The most common data types that are captured and accessed on a regular basis by authorized individuals are first and last name, middle initial, DOB, SSN, and address. This patient information falls into two classes: administrative and clinical. Clinical Information is used to diagnose, prescribe treatment and follow clinically the patient through his/her health care encounters. Administrative data is used to identify the veteran (SSN), correspond to/from (name and address), and determine eligibility (patient administrative info + SSA and IRS data) and for payment of healthcare.	Verbally	Written
Family Relation (spouse, children, parents, grandparents, etc)	VA File Database	with VistA. The information gathered will be used to determine eligibility and will not	Verbally	Written

Service Information	VA File Database	The LAN shares information with VistA. Military Service Information (Branch of service, discharge date, discharge type, service connection, medical conditions related to military service) This information is collected to assess eligibility for VA healthcare benefits, type of healthcare needed.	Verbally	Written
---------------------	------------------	--	----------	---------

Medical Information	VA File Database	The LAN shares information with the VistA system. VistA-Legacy applications used to meet a wide range of health care data needs. The system collects a wide range of personal medical information for clinical diagnosis, treatment, patient evaluation, and patient care. Common types of personal medical information would include lab test results, prescriptions, allergies, medical diagnosis, vital signs, etc. The information is used to treat and care for the veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of veterans.	Verbally	Written
---------------------	------------------	--	----------	---------

Criminal Record Information				
Guardian Information	VA File Database	The LAN shares information with the VistA system. Next of kin, DNR instructions, health care proxy designation. This information is used in the notification process and as required for medical decisions.	Verbally	Written
Education Information				

Benefit Information	The LAN shares information with the VistA system. Treatment notes, progress notes, clinical assessments, clinical diagnosis information is collected. Used in follow-up treatment and as part of the medical history. C&P examinations are also performed with information input into the CAPRI system utilized by VBA.	Verbally	Written
VA File Database			

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	VA Files / Databases (Identify file)	Mandatory	Authorized users may have documents that contain this information that reside on the network area storage server.

Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Voluntary	Authorized users may have documents that contain this information that reside on the network area storage server.
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory	Authorized users may have documents that contain this information that reside on the network area storage server.
Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory	Authorized users may have documents that contain this information that reside on the network area storage server.
Criminal Record Information				
Guardian Information	Yes	VA Files / Databases (Identify file)	Voluntary	Authorized users may have documents that contain this information that reside on the network area storage server.

Education Information

Benefit Information

Authorized users
may have
documents that
contain this
information that
reside on the
network area
storage server.

Yes

VA Files / Databases (Identify file)

Voluntary

Other (Explain)

Other (Explain)

Other (Explain)

(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	Other VAMCs and VBA	Yes	For the purpose of providing treatment and benefits	Both PII & PHI	VHA Handbook 1605.1 as referenced in local Privacy Policy
Other Veteran Organization		No		N/A	
Other Federal Government Agency	IRS, SSA, DOD	No	Income verification to determine if third party collection is possible and used to determine eligibility of care	Both PII & PHI	VHA Handbook 1605.1 as referenced in local Privacy Policy
State Government Agency	Medicaid, Licensing Boards, Courts	No	Used to determine eligibility of benefits and identification of authorized patient representatives	Both PII & PHI	VHA Handbook 1605.1 as referenced in local Privacy Policy
Local Government Agency		No		N/A	
Research Entity		No		N/A	
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:	VistA
Per responses in Tab 4, does the system gather information from an individual?	No
If information is gathered from an individual, is the information provided:	<input checked="" type="checkbox"/> Through a Written Request <input checked="" type="checkbox"/> Submitted in Person <input type="checkbox"/> Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	Yes

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?

No

if yes, please check all that apply:

- Drug/Alcohol Counseling Mental Health HIV
 Research Sickle Cell Other (Please Explain)

Describe process for authorizing access to this data.

Answer:

(FY 2011) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: Access to folders and data are restricted by permissions. The owner of the share grants access and access to shared data is authorized and approved by supervisors. Access to objects are controlled via access control lists and GPO settings.

How is data checked for completeness?

Answer: Information is reviewed before it is saved or action is taken.

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

Answer: Information is reviewed before it is saved or action is taken.

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

Answer: Information is reviewed before it is saved or action is taken.

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

Answer:

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: 75 years after the last episode of patient care.

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

Answer: For the treatment of patient care and according to RCS 10-1 and NARA.

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

Answer: The electronic final version of patient medical record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records Control Schedule 10-1, Item XLIII, 2.b (Page 190). At the present time, VistA Imaging retains all images.

Where are these procedures documented?

Answer: Center Memo 460-00.10 and RCS 10-1

How are data retention procedures enforced?

Answer: Records Management Officer of Health Information Management Service (HIMS) is responsible for developing policies, and procedures for effective and efficient records management throughout VHA. In addition, HIMS acts as the liaison between VHA and National Archives and Records Administration (NARA) on issues pertaining to records management practices and procedures. Chief of Health Information Management is

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

Yes

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

Answer:

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

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

No

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

Answer:

(FY 2011) PIA: Security

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

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

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

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

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

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

Answer:

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

If 'No' please describe why:

Answer:

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

Answer: SCA is conducted every 3 years or whenever there's a significant change. On the years that an SCA is not conducted, continuous monitoring is

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

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

Answer: (Other Risks)

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

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

Answer: (Other Controls)

PIA: PIA Assessment

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

Answer: Reconsideration of controls to mitigate misuse of information and reconsideration of security controls

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

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

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

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

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

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

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

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

Please add additional controls:

(FY 2011) PIA: Additional Comments

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

(FY 2011) PIA: VBA Minor Applications

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 | Care Management | ADP Planning (PlanMan) | x Authorization/ Subscription |
| x CAPRI | 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 | x CPT/ HCPCS Codes | 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 | Credentials Tracking | x Capacity Management Tools |
| x HINQ | x Engineering | x Discharge Summary | Clinical Info Resource Network |
| x IFCAP | x Event Capture | x Drug Accountability | x Clinical Monitoring System |
| x Imaging | 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 | External Peer Review | 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 |
| MICOM | x MyHealthEVet | x Health Level Seven | x Master Patient Index VistA |
| x NDBI | x National Drug File | x Hospital Based Home Care | x Missing Patient Reg (Original) A4EL |
| x NOIS | x Nursing Service | x Inpatient Medications | x Order Entry/ Results Reporting |
| x Oncology | x Occurrence Screen | x Integrated Patient Funds | x PCE Patient Care Encounter |
| x PAID | x Patch Module | x MCCR National Database | x Pharmacy Benefits Mangement |
| x Prosthetics | x Patient Feedback | x Minimal Patient Dataset | x Pharmacy Data Management |
| x QUASAR | x Police & Security | x National Laboratory Test | 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 | 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 | Survey Generator | x Security Suite Utility Pack | x Remote Order/ Entry System |
| x Unwinder | Utilization Review | x Shift Change Handoff Tool | x 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 | 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
		x

(FY 2011) PIA: Final Signatures

Facility Name: Region 4>VHA>VISN 04>Wilmington VAMC>LAN

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

Privacy Officer:	Miguel Sanchez	(302) 994-2511 x4750	miguel.sanchez@va.gov
------------------	----------------	-------------------------	--

Digital Signature Block

Information Security Officer:	Mary K. Jones	(302) 633-5551	mary.jones3@va.gov
-------------------------------	---------------	----------------	--

Digital Signature Block

System Owner/ Chief Information Officer:	Jack Galvin/Scott Viars	(518) 626-6244/(302) 644-5450	scott.viars@va.gov
--	-------------------------	-------------------------------	--

Digital Signature Block

Information Owner:	Charles M. Dorman, Director	(302) 633-5201	charles.dorman@va.gov
--------------------	-----------------------------	----------------	--

Digital Signature Block

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

Digital Signature Block

Date of Report: 1/18/11

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

Project Name: Region 4>VHA>VISN 04>Wilmington VAMC>LAN

(FY 2011) PIA: Final Signatures

Facility Name: Region 4>VHA>VISN 04>Wilmington VAMC>LAN

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

Privacy Officer:	Miguel Sanchez	(302) 994-2511 x4750	miguel.sanchez@va.gov
------------------	----------------	-------------------------	--

Miguel A. Sanchez 149191
 Digitally signed by Miguel A. Sanchez 149191
 DN: cn=Miguel A. Sanchez 149191 O = internal OU = people
 Date: 2011.02.11 07:37:48 -05'00'

Information Security Officer:	Mary K. Jones	(302) 633-5551	mary.jones3@va.gov
-------------------------------	---------------	----------------	--

MARY K JONES
 Digitally signed by MARY K JONES
 DN: o=Department of Veterans Affairs, ou=Dept. of Veterans Affairs, cn=MARY K JONES, email=mary.jones3@va.gov
 Date: 2011.02.10 17:18:13 -05'00'

System Owner/ Chief Information Officer:	Scott Viars	(518) 626-6244/(302) 644-5450	scott.viars@va.gov
--	-------------	-------------------------------	--

Jack Gr... Viars
 Digitally signed by Scott R. Viars
 DN: cn=Scott R. Viars C = US
 O = U.S. Government
 OU = Department of Veterans Affairs
 Date: 2011.02.11 13:46:24 -05'00'

Information Owner:	Charles T. Dorman, Director	(302) 633-5201	charles.dorman@va.gov
--------------------	-----------------------------	----------------	--

Charles T. Dorman, Director
 Digitally signed by Charles T. Dorman, Director
 Date: 2011.02.11 13:46:24 -05'00'

Other Titles: 0 0 0

Digital Signature Block

Date of Report: 1/18/11
 OMB Unique Project Identifier: 029-00-02-00-01-1120-00
 Project Name: Region 4>VHA>VISN 04>Wilmington VAMC>LAN