

(FY 2011) PIA: System Identification

Program or System Name: Veterans Health Administration (VHA) Leadership and Workforce Development System
 OMB Unique System / Application / Program Identifier (AKA: UPID #): Development>Region 2>VHA>VHA Leadership &

The Veterans Health Administration (VHA) Leadership and Workforce Development System (VHALWD) has 36 separate databases that contain information on people, positions, and organizations, work groups, workforce, workforce and leadership classes, workforce development programs and participation, personal development plans, supervisory levels, mentor and coach attributes, High Performance Development Model (HPDM) core competency, intern data, EEO reporting, succession planning, workforce planning, senior executive information, applicant tracking and recruitment, Executive Career Field (ECF) position and performance information, and education funding and programs. The VHA Executive Management Program consists of the functions that fall under the purview of the VHA Executive Resources Board (ERB) and the VHA Performance Review Board (PRB). Their functions include executive development, recruitment and placement, organizational analysis, succession planning, workforce planning, EEO and ADR assessment, workload tracking and reporting of human capital and HR, and individual and organizational performance assessment and recognition. The method used to collect this information is a proprietary system using relational database technology. Information from these databases are joined and expanded to inform programs and processes. This combination of information is used in the administration of talent management, VHA human capital objectives, and in the support of the ERB and PRB functions.

Description of System/ Application/ Program:

Facility Name: Central Arkansas Veterans Healthcare System

Title:	Name:	Phone:	Email:
Privacy Officer:	Angie Waddles	501-257-2972	angela.waddles@va.gov
Information Security Officer:	Billy W. Winkle	501-257-2084	billy.winkle@va.gov
System Owner/ Chief Information Officer:	Diana Rogers	817-385-3751	diana.rogers3@va.gov
Information Owner:	Diana Rogers	405-552-4346	diana.rogers3@va.gov
Other Titles:	James Hall	501-257-1531	james.hall@va.gov
Person Completing Document:	Gregory M. Williams	501-257-2006	gregory.williams6@va.gov
Other Titles:	N/A		

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY) N/A: First PIA

Date Approval To Operate Expires:

What specific legal authorities authorize this program or system:

161VA10A2 Veterans Health Administration Leadership and Workforce Development-Title 38, United States Code, section 501a

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

Approximately 25,500,000

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.

The system has been operational since March 2002

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

N/A: First PIA

If No, please explain:

Has a PIA been completed within the last three years?

No

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?

Does this system/application/program collect, store or disseminate PII/PHI data?

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

If there is no Personally Identifiable Information on your system , please complete TAB 2 & TAB 12. (See Comment for Definition of PII)

(FY 2011) PIA: System of Records

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

Yes

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

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

161VA10A2

2. Name of the System of Records:

161VA10A2 Veterans Health Administration (VHA)
Leadership and Workforce Development System

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

<http://govpulse.us/entries/2010/02/22/2010-3298/privacy-act-of-1974-system-of-records#id941396>

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?

No

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?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Paper & Electronic	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 the veteran.	Automated
Family Relation (spouse, children, parents, grandparents, etc)	Paper & Electronic	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 the veteran.	Automated
Service Information	Paper & Electronic	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 the veteran.	Automated
Medical Information	VA File Database	The information may be disclosed to a member of Congress, or a staff person acting for the member on behalf of the written request of the individual diagnosis and treatment of the veteran. Such as medical treatment information related to drug abuse, alcoholism or alcohol abuse, sickle cell anemia or infection with the human immunodeficiency virus.	Automated

VA may disclose information from this system of records to the Department of Justice (DoJ), either on VA's initiative or in response to DoJ's request for the information, after either VA or DoJ determines that such information is relevant to DoJ's representation of the United States or any of its components in legal proceedings before a court or adjudicative body, provided that, in each case, the agency also determines prior to disclosure that release of the records to DoJ is a use of the information contained in the records that is compatible with the purpose for which VA collected the records

Criminal Record Information

Electronic/File Transfer

Automated

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 the veteran.

Guardian Information

Paper & Electronic

Automated

Education Information

N/A

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 the veteran.

Benefit Information

VA File Database

Automated

Other (Explain)

Because VHALWD stores next-of-kin information and emergency contact information such as name and telephone number are collected from the veteran to use to contact other individuals in case of an emergency. In addition, insurance and employment information is available on the veteran for use in billing for care.

Automated

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	VA Files / Databases (Identify file)	Mandatory
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Mandatory
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory
Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory
Criminal Record Information	Yes	VA Files / Databases (Identify file)	Mandatory
Guardian Information	Yes	VA Files / Databases (Identify file)	Mandatory
Education Information	No	VA Files / Databases (Identify file)	Mandatory

Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory
Other (Explain)			
Other (Explain)			
Other (Explain)			

How is a privacy notice provided?

Automated via a link to the VA notice of Privacy policies

Automated via a link to the VA notice of Privacy policies

Automated via a link to the VA notice of Privacy policies

Automated via a link to the VA notice of Privacy policies

Automated via a link to the VA notice of Privacy policies

Automated

Automated via a link to the VA notice of Privacy policies

Automated via a link to the VA notice of Privacy policies

Additional Comments

Automated via a link to the VA notice of Privacy policies

Automated via a link to the VA notice of Privacy policies

Automated via a link to the VA notice of Privacy policies

Automated via a link to the VA notice of Privacy policies

Automated via a link to the VA notice of Privacy policies

Automated via a link to the VA notice of Privacy policies

Automated via a link to the VA notice of Privacy policies

Automated via a link to the VA notice of Privacy policies

(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			Organization/Position Assignment of Employees		Approval by Chief of HR, Network Directors, DVA HR&A, WMC and HTM office.
	VHA, DVA, NCA, VBA	Yes		PII	
Other Veteran Organization	NA	No		N/A	
Other Federal Government Agency	NA	No		N/A	
State Government Agency	NA	No		N/A	
Local Government Agency	NA	No		N/A	
Research Entity	NA	No		N/A	
Other Project / System		No		N/A	
Other Project / System		No		N/A	
Other Project / System		No		N/A	

(FY 2011) PIA: Access to Records

Does the system gather information from another system? Yes

Please enter the name of the system: Active Directory, Nature of Action, Employee and Payroll

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? No

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

if yes, please check all that apply:

Describe process for authorizing access to this 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: Processes are in place to ensure data collection of only required data. Data is entered electronically with the use of automated forms that request only the data necessary eliminating the collection of unnecessary data.

How is data checked for completeness?

Answer: Business rules, data review by data owners relational databases and confirmation by end-users.

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

Answer: Data is updated with each instance of personnel actions, personnel notifications, PAID transactions, Nature of Actions and payrolls processing. PAID data is updated eight times a pay period. Data is verified and updated at the time an SF52 action is generated.

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

Answer: Supervisors verify that the autopopulated SF52 is accurate before submission for processing by HR; HR verifies that: the action is valid, employee and position information is accurate, coding and processing follow policy, guidelines, regulations and HDMLs, ensuring accurate input and results after processing are accurate.

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: Documents are required for retention following the guidance in Guide to Personnel Recordkeeping (GPR) which clearly outlines documents required for long term retention and/or transfer. The Title V of the Code of Federal Regulations (CFR), § 293.405 which explains the retention period for SES and non-SES performance rating of record. Finally, the eOPF Master Forms List identifies forms designated as Permanent, Temporary, and Agency specific documents for both Title V and non-Title V organizations for those agencies that have migrated to eOPF. The retention period is dependent on the type of data and the intended use. VA Records Control Schedule 10-1 (page 8) has Records Management Responsibilities for developing policies and procedures for effective and efficient records management throughout VHA. Program officials are responsible for creating, maintaining, protecting, and disposing of records in their program area in accordance with National Archives and Records Administration (NARA) regulations and VA policy. All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures.

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

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

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

Answer: Applicable federal regulatory requirements will be followed for eliminating or disposing of data.

Where are these procedures documented?

Answer: VA Handbook 6300; Record Control Schedule 10-1

How are data retention procedures enforced?

Answer: Procedures will be enforced using technical and managerial control mechanisms.

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: Procedures which are consistent with the provisions of Federal Information Security Management Act (FISMA) as well as guidance issued by the Office of Management & Budget (OMB), the National Institute of Standards & Technology (NIST), & Federal Information Processing Standards (FIPS). In addition, OI&T Field Security Operations administers and manages Department-wide security solutions, such as anti-virus protection, authentication, vulnerability scanning & penetration testing, & intrusion detection systems, and incident response (800-61). The Project Manager ensures that CIO-provided security directives are integrated into the project's security plan & implemented by VA & contractor staff throughout the project. Funding needs are dependent on IT security requirements identified in the system development life cycle (800-64) (i.e. risk assessments (800-30), certification and accreditation (800-37 and 80053)), with consistent review and ongoing assessment of security weaknesses and mitigation of any weaknesses identified.

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 type="checkbox"/> Chemical/Biological Contamination | <input checked="" type="checkbox"/> Data Integrity Loss | <input checked="" type="checkbox"/> Identity Theft |
| <input checked="" type="checkbox"/> Blackmail | <input checked="" type="checkbox"/> Denial of Service Attacks | <input checked="" type="checkbox"/> Malicious Code |
| <input checked="" type="checkbox"/> Bomb Threats | <input checked="" type="checkbox"/> Earthquakes | <input checked="" type="checkbox"/> Power Loss |
| <input checked="" type="checkbox"/> Burglary/Break In/Robbery | <input checked="" type="checkbox"/> Eavesdropping/Interception | <input checked="" type="checkbox"/> Sabotage/Terrorism |
| <input type="checkbox"/> Cold/Frost/Snow | <input checked="" type="checkbox"/> Errors (Configuration and Data Entry) | <input checked="" type="checkbox"/> Storms/Hurricanes |
| <input checked="" type="checkbox"/> Communications Loss | | <input checked="" type="checkbox"/> Substance Abuse |

- Cold/Frost/Snow
- Communications Loss
- Computer Intrusion
- Computer Misuse
- Data Destruction

Answer: (Other Risks)

- Errors (Configuration and Data Entry)
- Fire (False Alarm, Major, and Minor)
- Flooding/Water Damage
- Fraud/Embezzlement

- Storms/Hurricanes
- Substance Abuse
- Theft of Assets
- Theft of Data
- Vandalism/Rioting

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

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

Answer: (Other Controls)

PIA: PIA Assessment

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

Answer:

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 VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow NIST SP800-53 moderate impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of this facility' common security controls. These issues are identified and described in the system security plans for the individual information systems.

Please add additional controls:

(FY 2011) PIA: Additional Comments

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

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?
--

Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial	BCMA Contingency Machines	Automated Medical Information Exchange II (AIME II)
Appraisal System	Benefits Delivery Network (BDN)	Automated Medical Information System (AMIS)290
ASSISTS	Centralized Property Tracking System	Automated Standardized Performance Elements Nationwide (ASPEN)
Awards	Common Security User Manager (CSUM)	Centralized Accounts Receivable System (CARS)
Awards	Compensation and Pension (C&P)	Committee on Waivers and Compromises (COWC)
Baker System	Control of Veterans Records (COVERS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)	Control of Veterans Records (COVERS)	Compensation & Pension Training Website
BDN Payment History	Control of Veterans Records (COVERS)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
BIRLS	Courseware Delivery System (CDS)	Distribution of Operational Resources (DOOR)
C&P Payment System	Dental Records Manager	Educational Assistance for Members of the Selected Reserve Program CH 1606
C&P Training Website	Education Training Website	Electronic Performance Support System (EPSS)
CONDO PUD Builder	Electronic Appraisal System	Enterprise Wireless Messaging System (Blackberry)
Corporate Database	Electronic Card System (ECS)	Financial Management Information System (FMI)
Data Warehouse	Electronic Payroll Deduction (EPD)	Hearing Officer Letters and Reports System (HOLAR)
EndoSoft	Eligibility Verification Report (EVR)	inquiry Routing Information System (IRIS)
FOCAS	Fiduciary Beneficiary System (FBS)	Modern Awards Process Development (MAP-D)
Inforce	Fiduciary STAR Case Review	Personnel and Accounting Integrated Data and Fee Basis (PAID)
INS - BIRLS	Financial and Accounting System (FAS)	Personal Computer Generated Letters (PCGL)
Insurance Online	Insurance Unclaimed Liabilities	Personnel Information Exchange System (PIES)
Insurance Self Service	Inventory Management System (IMS)	Personnel Information Exchange System (PIES)
LGY Home Loans	LGY Centralized Fax System	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing	Loan Service and Claims	Purchase Order Management System (POMS)
Mobilization	Loan Guaranty Training Website	Reinstatement Entitlement Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Assistant	Service Member Records Tracking System
Omnicell	National Silent Monitoring (NSM)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Powerscribe Dictation System	Systematic Technical Accuracy Review (STAR)
RAI/MDS	Rating Board Automation 2000 (RBA2000)	Training and Performance Support System (TPSS)
Right Now Web	Rating Board Automation 2000 (RBA2000)	VA Online Certification of Enrollment (VA-ONCE)
SAHSHA	Rating Board Automation 2000 (RBA2000)	VA Reserve Educational Assistance Program
Script Pro	Records Locator System	Veterans Appeals Control and Locator System (VACOLS)
SHARE	Review of Quality (ROQ)	Veterans Assistance Discharge System (VADS)
SHARE	Search Participant Profile (SPP)	Veterans Exam Request Info System (VERIS)
SHARE	Spinal Bifida Program Ch 18	Veterans Service Representative (VSR) Advisor
Sidexis	State Benefits Reference System	Vocational Rehabilitation & Employment (VR&E) CH 31
Synquest	State of Case/Supplemental (SOC/SSOC)	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

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

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

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

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

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

(FY 2011) PIA: Minor Applications

Which of these are sub-components of your system?

1184 Web

ENDSOFT
Enterprise Terminology Server &
VHA Enterprise Terminology
Services

RAFT
RALS

A4P

(FY 2011) PIA: Final Signatures

Facility Name: Veterans Health Administration (VHA) Leadership and Workforce Development System

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

Privacy Officer:	Angie Waddles	501-257-2972	angela.waddles@va.gov
------------------	---------------	--------------	-----------------------

Angie Waddles

Information Security Officer:	Billy W. Winkle	501-257-2084	billy.winkle@va.gov
-------------------------------	-----------------	--------------	---------------------

Billy W. Winkle 8/2/2011

System Owner/ Chief Information Officer:	Diana Rogers	817-385-3751	diana.rogers3@va.gov
--	--------------	--------------	----------------------

Diana Rogers 7-20-11

Information Owner:	Diana Rogers	405-552-4346	diana.rogers3@va.gov
--------------------	--------------	--------------	----------------------

Diana Rogers 7-20-11

Other Titles:	James Hall	501-257-1531	james.hall@va.gov
---------------	------------	--------------	-------------------

Jim Hall 7-20-2011

Date of Report: 1/0/00

Development>Region 2>VHA>VHA
Leadership & Workforce
Development (VHALWD)

OMB Unique Project Identifier