

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:	OA&L>DALC>ROES		
OMB Unique System / Application / Program Identifier	(AKA: UPID #):		
Description of System/ Application/ Program:	The Denver Acquisition & Logistics Center is a field program of the VA Office of Acquisition & Logistics (OAL). The DALC ROES/VistA system supports organizational business processes through information systems and automation. ROES/VistA optimizes order fulfillment systems and manages VA national data repositories supporting clinical programs of DALC customers. In doing so, ROES enables DALC mission objectives in directly supporting clinical practice and patient care delivered by its stakeholder programs.		
Facility Name:	Denver Acquisition & Logistics Center (Station 791)		
Title:	Name:	Phone:	Email:
Privacy Officer:	Regina Krawiec	303-914-5150	regina.krawiec@va.gov
Information Security Officer:	Scott Lewis	708-786-5144	scott.lewis1@va.gov
System Owner/ Chief Information Officer:	Kevin Quitmeyer	303-914-5160	kevin.quitmeyer@va.gov
Information Owner:	Kevin Quitmeyer	303-914-5160	kevin.quitmeyer@va.gov
Other Titles:			
Person Completing Document:	Regina Krawiec		
Other Titles:			
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	12/2009		
Date Approval To Operate Expires:	03/2012		

Collection and use are authorized under Title 38, USC Section 7301(a). In addition, VA has been delegated authority by the General Services Administration to manage Federal Supply Service (FSS) Schedule 65 contracts and contracts for the portion of Schedule 65 that pertains to medical equipment. Within the VA Acquisition and Logistics program, the DALC has authority to establish contracts and manage associated records for designated VHA clinical programs. Products and services are provided based on entitlements set forth in VHA Handbook 1173. The e-gov Act authorizes retention of personal information for the designated purposes in serving the public.

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:

Personal information is stored on approximately 1.5 million individuals.

20 System Identification 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.

In performance of the DALC mission, operational processes have existed and records have been maintained for 60 years. Initial implementation of a comprehensive IT/automated system occurred in 1991. Significant advances in implementation of automated systems occurred in 1995 and 2003, with continuing advances under development.

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):

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):

79VA19; 121VA19

2. Name of the System of Records:

Veterans Health Information Systems Technology Architecture (Vista)-VA; National Patient Databases-VA

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

<http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm>

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?

Yes

Does the System of Records Notice require modification or updating?

No

(Please Select Yes/No)

Is PII collected by paper methods?

Yes

Is PII collected by verbal methods?

Yes

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

Yes

Proximity and Timing: Is the privacy notice provided at the time of data collection?

Yes

Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

Yes

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

Yes

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

Yes

(FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	VA File Database	Health care	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)				
Service Information	VA File Database	Health care	Written	Written
Medical Information	VA File Database	Health care	Written	Written
Criminal Record Information				
Guardian Information				
Education Information				
Benefit Information	VA File Database	Health care	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	VA Files / Databases (Identify file)	Mandatory	Source: VA corporate VistA/CPRS electronic health records

Family Relation (spouse, children,
parents, grandparents, etc)

Service Information

Yes

VA Files / Databases (Identify file)

Mandatory

Source: VA
corporate
VistA/CPRS
electronic health
records

Medical Information

Yes

VA Files / Databases (Identify file)

Mandatory

Source: VA
corporate
VistA/CPRS
electronic health
records

Criminal Record Information

Guardian Information

Education Information

Benefit Information

Yes

VA Files / Databases (Identify file)

Mandatory

Source: VA
corporate
VistA/CPRS
electronic health
records

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 Veteran Organization					
Other Federal Government Agency	Department of Defense and Indian Health Service	Yes	One designated application is accessible by authorized healthcare providers in other Federal agencies. When working within this application, end users have access to their own patients' personal identifying information and medical information supporting their patient care needs.	N/A	Other government agency (OGA) healthcare providers access information originally provided by them and stored on the DALC/ROES system.
State Government Agency					
Local Government Agency					
Research Entity					

Other Project / System	VHA Prosthetic and Sensory Aids Program (113)	No	<p>Information on patient-specific DALC orders is shared for inclusion in a PSAS patient 2319 record. Personal information shared consists of name and SSN. Medical information shared consists of product name and HCPCS code. The information is shared for purposes of assisting in maintenance of data accuracy and budget management by the PSAS program.</p>	Both PII & PHI	<p>Internal sharing within the VA healthcare system. Data shared via electronic interface.</p>
Other Project / System	VA Decision Support System	No	<p>Personal information shared consists of SSN and four characters of last name. Medical/eligibility information consists of HCPCS code and VA eligibility (SC/NSC/etc.) code. The information is shared for purposes of aggregate data analysis and management decision support.</p>	Both PII & PHI	<p>Data shared via electronic data extract.</p>

Other Project / System

VA Enrollee Healthcare
Projection Model

No

Personal/medical
information shared
consists of SSN and HCPCS
code. The information is
shared for purposes of
data analysis and
projections affecting VA
resource allocation in
upcoming years.

Both PII & Data shared via electronic
PHI data extract.

(FY 2011) PIA: Access to Records

Does the system gather information from another system? Yes

Please enter the name of the system: Individual VAMC VistA systems

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: Some product orders generated at the DALC are transmitted electronically to commercial vendors/trading partners. For these orders, the products ordered are custom-manufactured for a specific patient, in which case it is necessary to inform the manufacturer of the individual for whom the product is being ordered/manufactured. This applies to hearing devices, which are serialized devices. The information exchange with commercial vendors is necessary to ensure issue of manufactured devices to the proper patients and maintenance of accurate warranty information. This information exchange is governed by Business Associate Agreements in place implementing HIPAA and Privacy Act protections. Purchase transactions, including truncated segments of patient name and SSN, are transmitted to the VA Electronic Data Interchange (EDI) system, which acts as an intermediary translation partner in this electronic commerce process.

(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: Interfaces and applications are constructed to obtain only that data which is necessary for DALC mission objectives. Data fields collected through local VAMC/Vista interfaces, online forms, and paper forms are limited to those necessary for DALC processing.

How is data checked for completeness?

Answer: Incoming data elements are validated by requirements implemented in the DALC data dictionary.

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

Answer: Data are associated with verified episodes of care or reported geographical movements to ensure that they are current. Data are also periodically compared to that available from other authoritative sources within VA, such as the Health Eligibility Center (HEC) and Financial Services Center (FSC).

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

Answer: Data are accepted only from authoritative VA sources or on a limited basis from individual subjects.

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: The data is retained permanently.

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

Answer: Patient records and medical device information must remain available well beyond conclusion of the patient's treatment by VA.

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

Answer: N/A

Where are these procedures documented?

Answer: N/A

How are data retention procedures enforced?

Answer: N/A

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

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: The program undergoes Systems Certification & Accreditation according to NIST guidance and at established intervals as required by VA policy, culminating with a final Authority to Operate.

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 checked="" 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 checked="" 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 type="checkbox"/> Flooding/Water Damage | <input type="checkbox"/> Theft of Assets |
| <input 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)

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Access Control | <input checked="" type="checkbox"/> Contingency Planning | <input checked="" type="checkbox"/> Personnel Security |
| <input checked="" type="checkbox"/> Audit and Accountability | <input checked="" type="checkbox"/> Identification and Authentication | <input checked="" type="checkbox"/> Physical and Environmental Protection |
| <input checked="" type="checkbox"/> Awareness and Training | <input checked="" type="checkbox"/> Incident Response | <input checked="" type="checkbox"/> Risk Management |
| <input checked="" type="checkbox"/> Certification and Accreditation Security Assessments | | |
| <input checked="" type="checkbox"/> Configuration Management | <input checked="" type="checkbox"/> 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:

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)

- | | |
|-------------------------------------|---|
| <input type="checkbox"/> | 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. |
| <input checked="" type="checkbox"/> | The potential impact is moderate if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. |
| <input type="checkbox"/> | 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)

- | | |
|-------------------------------------|--|
| <input type="checkbox"/> | 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. |
| <input checked="" type="checkbox"/> | The potential impact is moderate if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals. |
| <input type="checkbox"/> | 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)

- | | |
|-------------------------------------|--|
| <input type="checkbox"/> | 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. |
| <input checked="" type="checkbox"/> | The potential impact is moderate if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals. |
| <input type="checkbox"/> | 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.

2. System Identification - Stage of System:

Since the system supports a dynamic business process environment, the system itself is subject to additional development/implementation activities to maintain alignment with that business environment.

4. Notice:

Individuals are notified of the governing VA Privacy Policy at the time of patient care encounters at VHA facilities. Notification procedures are determined and carried out by VHA and/or local facility procedures regarding notification of information collection and patient privacy protections.

5. Data Sharing & Access - Access to Records:

Information is collected from each individual VAMC VistA database to enable addition of eligible veterans to the DALC database, confirmation of DALC veteran records based on veteran identity, and verification of veteran eligibility to receive DALC products and services. Veteran mailing address is collected/updated based on veteran-provided information to ensure accuracy of product delivery. Veteran e-mail address is collected/updated based on voluntary veteran-provided information to allow for timely communication with the veteran regarding product delivery.

Information is collected from VAMC VistA systems when ROES actions are initiated by clinicians. This information is passed to the ROES web application during ROES session setup. Information related to patient audiometric assessments is also collected using a VAMC-resident application. In finalizing the audiometric assessment/data collection, information is stored locally on the VAMC system and simultaneously transmitted to the DALC in a designated national repository.

Information is collected from VA clinical providers via the DALC-hosted ROES application. The core version of ROES is accessible only from internal VA systems and only by using a specified 'entry point' executable file implemented on VAMC systems by authorized VHA IT staff.

(FY 2011) PIA: VBA Minor Applications

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

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

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

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

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

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

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

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

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

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

ASISTS	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	x Capacity Management Tools
x HINQ	x Engineering	Discharge Summary	Clinical Info Resource Network
x IFCAP	Event Capture	Drug Accountability	Clinical Monitoring System
Imaging	Extensible Editor	EEO Complaint Tracking	Enrollment Application System
x Kernal	Health Summary	x Electronic Signature	x Equipment/ Turn-in Request
x 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
x Mailman	List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine	Mental Health	Generic Code Sheet	Interim Mangement Support
MICOM	MyHealthEVet	x 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
x PAID	Patch Module	MCCR National Database	Pharmacy Benefits Mangement
Prosthetics	Patient Feedback	Minimal Patient Dataset	Pharmacy Data Management
x QUASER	Police & Security	National Laboratory Test	Pharmacy National Database
x RPC Broker	Problem List	Network Health Exchange	Pharmacy Prescription Practice
x 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
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	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	RAFT
A4P	Enterprise Terminology Server & VHA Enterprise Terminology Services	RALS

(FY 2011) PIA: Final Signatures

Facility Name: OA&L>DALC>ROES

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

Privacy Officer:	Regina Krawiec	303-914-5150	regina.krawiec@va.gov
------------------	----------------	--------------	-----------------------

Digital Signature Block

Information Security Officer:	Scott Lewis	708-786-5144	scott.lewis1@va.gov
-------------------------------	-------------	--------------	---------------------

Digital Signature Block

System Owner/ Chief Information Officer:	Kevin Quitmeyer	303-914-5160	kevin.quitmeyer@va.gov
--	-----------------	--------------	------------------------

Digital Signature Block

Information Owner:	Kevin Quitmeyer	303-914-5160	kevin.quitmeyer@va.gov
--------------------	-----------------	--------------	------------------------

Digital Signature Block

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

Digital Signature Block

Date of Report: 12/29/10

OMB Unique Project Identifier 0

Project Name OA&L>DALC>ROES