

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:	Development > CDCO > AITC > VA > EIE > ETS (Enterprise Testing Services)		
OMB Unique System / Application / Program Identifier	(AKA: UPID #):	none in SMART	
Description of System/ Application/ Program:	A 252 server Pre-Production test lab that will support HealtheVet, Legacy Vista, and WAN emulation testing in support of OED and EIE efforts for improved testing and system implementation procedures.		
Facility Name:	Austin Information Technology Center (AITC)		
Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	512-326-6217	Amy.Howe1@va.gov
Information Security Officer:	Craig Heitz	612-725-2132	Craig.heitz@va.gov
System Owner/ Chief Information Officer:	John Rucker	512-326-6422	John.Rucker@va.gov
Information Owner:			
Other Titles:			
Person Completing Document:	Oswaldo Melendez	512-326-6247	Oswaldo.melendez@va.gov
Other Titles:			
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)			Initial PIA
Date Approval To Operate Expires: No ATO; First C&A effort			n/a
What specific legal authorities authorize this program or system:	OI&T Mandate		
What is the expected number of individuals that will have their PII stored in this system:	Approximately 100		
Identify what stage the System / Application / Program is at:	Development/Acquisition		
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.	12/2011		
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?	N/A: First PIA		
Date of Report (MM/YYYY):	03/2011		

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

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

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

(FY 2011) PIA: System of Records

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

Yes

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

- | | |
|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| 1. All System of Record Identifier(s) (number): | 121VA19 |
| 2. Name of the System of Records: | National Patient Databases - VA |
| 3. Location where the specific applicable System of Records Notice may be accessed (include the URL): | http://vawww.vhaco.va.gov/privacy/SystemofReco |

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?

No

Is a Privacy notice provided?

No

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

No

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

No

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

No

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

No

(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)	Electronic/File Transfer	N/A - Information is system generated	N/A	N/A
Family Relation (spouse, children, parents, grandparents, etc)	N/A			
Service Information	Electronic/File Transfer	N/A - Information is system generated	N/A	N/A
Medical Information	Electronic/File Transfer	N/A - Information is system generated	N/A	N/A
Criminal Record Information	N/A			
Guardian Information	N/A			
Education Information	N/A			
Benefit Information	N/A			
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	Data is collected from files
Family Relation (spouse, children, parents, grandparents, etc)	No			
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory	Data is collected from files
Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory	Data is collected from files
Criminal Record Information	No			
Guardian Information	No			
Education Information	No			
Benefit Information	No			
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	VHA, OED, ESE, AITC	Yes	PHI & PII. Used for creating duplicate production environment for testing and implementation of new releases, troubleshooting, etc.	Both PII & PHI	VA Directive 6500
Other Veteran Organization		No			
Other Federal Government Agency		No			
State Government Agency		No			
Local Government Agency		No			
Research Entity		No			
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:	HealtheVet, Legacy 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 type="checkbox"/> Through a Written Request <input 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? ETS will also provide a Routine Support Disaster Recovery solution.		Yes

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?		No
if yes, please check all that apply:	<input type="checkbox"/> Drug/Alcohol Counseling <input type="checkbox"/> Mental Health <input type="checkbox"/> HIV <input type="checkbox"/> Research <input type="checkbox"/> Sickle Cell <input type="checkbox"/> 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: ETS Lab is being system up for system specific data; HealtheVet, Legacy Vista, and any WAN Emulation data.

How is data checked for completeness?

Answer: ETS Lab capability for real-time monitoring and mirrored HealtheVet & Legacy environment.

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

Answer: ETS Lab capability for real-time monitoring and mirrored HealtheVet & Legacy environment.

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

Answer: ETS Lab capability for real-time monitoring and mirrored HealtheVet & Legacy environment.

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 retention process is based upon the Department of Veterans Affairs Record Control Schedule 10-1, Revised June 28, 2006. Data will be retained until 3 years after last episode of care. It will then be converted to an archived system but will be retrievable if/when the patient returns for further treatment. Data in the archived system will be retained 75 years after the veterans last episode of care.

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

Answer: DVA Record Control Schedule 10-1, revised June 28, 2006, specifies how long patient data will be maintained.

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

Answer: Data will be purged 75 years after the veterans's last episode of care.

Where are these procedures documented?

Answer: VA Handbook 6300.1, Records Management Procedures explains the Records Control Schedule procedures.

How are data retention procedures enforced?

Answer: VA Directive 6300, contains the policies and responsibilities for VA's records and information management program. Procedures are enforced by Records Management Staff and VA Records Officers.

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 ETS Lab is going through the FISMA mandated Certification and Accreditation process.

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 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 checked="" 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 checked="" 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 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 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 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: None.

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 checked="" 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 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? No, first assessment.

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

Please add additional controls:

(FY 2011) PIA: Additional Comments

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

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?

Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial	BCMA Contingency Machines	Automated Medical Information Exchange II (AIME II)
Appraisal System	Benefits Delivery Network (BDN)	Automated Medical Information System (AMIS)290
ASSISTS	Centralized Property Tracking System	Automated Standardized Performace Elements Nationwide (ASPEN)
Awards	Common Security User Manager (CSUM)	Centralized Accounts Receivable System (CARS)
Awards	Compensation and Pension (C&P)	Committee on Waivers and Compromises (COWC)
Baker System	Control of Veterans Records (COVERS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)	Control of Veterans Records (COVERS)	Compensation & Pension Training Website
BDN Payment History	Control of Veterans Records (COVERS)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
BIRLS	Courseware Delivery System (CDS)	Distribution of Operational Resources (DOOR)
C&P Payment System	Dental Records Manager	Educational Assistance for Members of the Selected Reserve Program CH 1606
C&P Training Website	Education Training Website	Electronic Performance Support System (EPSS)
CONDO PUD Builder	Electronic Appraisal System	Enterprise Wirelless Messaging System (Blackberry)
Corporate Database	Electronic Card System (ECS)	Financial Management Information System (FMI)
Data Warehouse	Electronic Payroll Deduction (EPD)	Hearing Officer Letters and Reports System (HOLAR)
EndoSoft	Eligibility Verification Report (EVR)	Inquiry Routing Information System (IRIS)
FOCAS	Fiduciary Beneficiary System (FBS)	Modern Awards Process Development (MAP-D)
Inforce	Fiduciary STAR Case Review	Personnel and Accounting Integrated Data and Fee Basis (PAID)
INS - BIRLS	Financial and Accounting System (FAS)	Personal Computer Generated Letters (PCGL)
Insurance Online	Insurance Unclaimed Liabilities	Personnel Information Exchange System (PIES)
Insurance Self Service	Inventory Management System (IMS)	Personnel Information Exchange System (PIES)
LGY Home Loans	LGY Centralized Fax System	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing	Loan Service and Claims	Purchase Order Management System (POMS)
Mobilization	Loan Guaranty Training Website	Reinstatement Entitelment Program for Survivors (REAPS)
Montgomery Gi Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Asisstant	Service Member Records Tracking System
Omicell	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	Telecare Record Manager	Web Automated Folder Processing System (WAFPS)
VBA Training Academy	VBA Enterprise Messaging System	Web Automated Reference Material System (WARMS)
Veterans Canteen Web	Veterans On-Line Applications (VONAPP)	Web Automated Verification of Enrollment
VIC	Veterans Service Network (VETSNET)	Web-Enabled Approval Management System (WEAMS)
VR&E Training Website	Web Electronic Lender Identification	Web Service Medical Records (WebSMR)
Web LGY		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 Appl

Which of these are sub-components of your system?

ASISTS	Beneficiary Travel	Accounts Receivable
Bed Control	Care Management	ADP Planning (PlanMan)
CAPRI	Care Tracker	Bad Code Med Admin
CMOP	Clinical Reminders	Clinical Case Registries
Dental	CPT/ HCPCS Codes	Clinical Procedures
Dietetics	DRG Grouper	Consult/ Request Tracking
Fee Basis	DSS Extracts	Controlled Substances
GRECC	Education Tracking	Credentials Tracking
HINQ	Engineering	Discharge Summary
IFCAP	Event Capture	Drug Accountability
Imaging	Extensible Editor	EEO Complaint Tracking
Kernal	Health Summary	Electronic Signature
Kids	Incident Reporting	Event Driven Reporting
Lab Service	Intake/ Output	External Peer Review
Letterman	Integrated Billing	Functional Independence
Library	Lexicon Utility	Gen. Med. Rec. - I/O
Mailman	List Manager	Gen. Med. Rec. - Vitals
Medicine	Mental Health	Generic Code Sheet
MICOM	MyHealthEVet	Health Level Seven
NDBI	National Drug File	Hospital Based Home Care
NOIS	Nursing Service	Inpatient Medications
Oncology	Occurrence Screen	Integrated Patient Funds
PAID	Patch Module	MCCR National Database
Prosthetics	Patient Feedback	Minimal Patient Dataset
QUASER	Police & Security	National Laboratory Test
RPC Broker	Problem List	Network Health Exchange
SAGG	Progress Notes	Outpatient Pharmacy
Scheduling	Record Tracking	Patient Data Exchange
Social Work	Registration	Patient Representative
Surgery	Run Time Library	PCE Patient/ HIS Subset
Toolkit	Survey Generator	Security Suite Utility Pack
Unwinder	Utilization Review	Shift Change Handoff Tool
VA Fileman	Visit Tracking	Spinal Cord Dysfunction
VBECS	VistALink Security	Text Integration Utilities
VDEF	Women's Health	VHS & RA Tracking System
VistALink		Voluntary Timekeeping

Applications

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

Explain any minor application that are associated with your installation that does not have a 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?

oes not appear in the list above. Please provide

--

--

--

(FY 2011) PIA: Minor Applications

Which of these are sub-components of your system?

1184 Web	Agent Cashier	Administrative Data Repository (ADR)
A4P	Air Fortress	Automated Access Request
ADT	Auto Instrument	Bed Board Management System
BDN 301	Cardiff Teleform	Cardiology Systems (stand alone servers from the network)
CP&E	CHECKPOINT	Clinical Data Repository/Health Data Repository
DRM Plus	Data Innovations	Combat Veteran Outreach
DSIT	DELIVEREX	Committee on Waiver and Compromises
ENDSOFT	DSS Quadramed	Crystal Reports Enterprise
EYECAP	EKG System	DICTATION-Power Scribe
Genesys	ePROMISE	EDS Whiteboard (AVJED)
ICB	Lynx Duress Alarm	Embedded Fragment Registry
KOWA	Mumps AudioFAX	Enterprise Terminology Server & VHA Enterprise Terminology Services
MHTP	Onvicord (VLOG)	Financial and Accounting System (FAS)
NOAHLINK	P2000 ROBOT	Financial Management System (FMS)
Omnicell	PACS database	Health Summary Contingency
Optifill	PIV Systems	Microsoft Active Directory
PICIS OR	Remedy Application	Microsoft Exchange E-mail System
Q-Matic	Traumatic Brain Injury	Military/Vet Eye Injury Registry
RAFT	VAMedSafe	Personal Computer Generated Letters
RALS	VBA Data Warehouse	QMSI Prescription Processing
SAN	VHAHUNAPP1	Scanning Exam and Evaluation System
Sentillion	VHAHUNFPC1	Tracking Continuing Education
Stellant	VISTA RAD	VA Conference Room Registration
Stentor	Whiteboard	

Explain any minor application that are associated with your installation that does not appear in the list above. Please

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: Final Signatures

Facility Name: AITC

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

Privacy Officer:	Amy Howe	512-326-6217	Amy.Howe1@va.gov
------------------	----------	--------------	--------------------------------------------------------

Digital Signature Block

Information Security Officer:

Digital Signature Block

System Owner/Chief Information Officer:	John Rucker	512-326-6422	John.Rucker@va.gov
-----------------------------------------	-------------	--------------	------------------------------------------------------------


Digital Signature Block

Information Owner:

Digital Signature Block

Other Titles:

Digital Signature Block

Date of Report:

OMB Unique Project Identifier

Project Name

(FY 2011) PIA: Final Signatures

Facility Name: Development > CDCO > AITC > VA > EIE > ETS (Enterprise Testing Services)

Title: Name: Phone: Email:

Privacy Officer: Amy Howe 512-326-6217 Amy.Howe1@va.gov

Digital Signature Block

Information Security Officer: Craig Heitz 612-725-2132 Craig.heitz@va.gov


Digital Signature Block
24 May 2011

System Owner/ Chief Information Officer: John Rucker 512-326-6422 John.Rucker@va.gov

Digital Signature Block

Date of Report: 03/2011

OMB Unique Project Identifier: none in SMART

Development > CDCO > AITC > VA >

EIE > ETS (Enterprise Testing

Services)

Project Name