

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. More information can be found by reading VA 6508.

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 Privacy Impact Assessment Handbook 6202.2 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 Handbook 6202.2.
- 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 Handbook 6202.2 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

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.

(FY 2011) PIA: System Identification

Program or System Name: Development > CDCO > AITC > OAL > VLTrader
 OMB Unique System / Application / Program Identifier (AKA: UPID #): Not in SMART

VLTrader encrypts EDI (electronic data interchange) transaction data and sends the information to trading partners for purchases.
 The E-Commerce/E-Business EDI and Server Operations (EC/EB EDISO) is a field program of the VA Office of Information & Technology (OI&T). The EDISO functions in the role of providing support for EDI processing activities in use by various VA facilities. The EC/EB EDISO performs processing of procurement data in support of the VHA healthcare system and other VA organizational elements and subsequent transmission of such data to EDI trading partners (vendors) and Value Added Networks (Vans). In doing so, IT systems are relied on prominently to ensure accuracy and efficiency of business functions. EC/EB EDISO business operations are automated to a significant extent. Various individual systems and applications optimize automation, facilitate order entry, and data management functions for the EC/EB EDISO and its customers/stakeholders.

Description of System/ Application/ Program:

Facility Name: Austin Information Technology Center

Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	326-6217	Amy.Howe1@va.gov
Information Security Officer:	Charles Aponte	326-6593	Charles.Aponte2@va.gov
System Owner/ CIO	Judy Downing	326-6000	Judy.Downing@va.gov
Information Owner:	Tammy Watson	202-461-6126	Tammy.Watson@va.gov
Other Titles: Supervisory IT Specialist	Chris Kelly	326-6464	Chris.Kelly@va.gov
Person Completing Document:	Megan Juckett	326-6890	Megan.Juckett@va.gov

Other Titles:

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

N/A

Date Approval To Operate Expires:

In development.

What specific legal authorities authorize this program or system:

VA 6500 pg 65 Paragraph O

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

1.2 million

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.

09/2010

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?

N/A: First PIA

Date of Report (MM/YYYY):

09/2010

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

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

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

(FY 2011) PIA: System of Records

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

[Yes](#)

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

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

79VA19

2. Name of the System of Records:

Veterans Health Information Systems and Technology Architecture (VistA) Records-VA

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

http://www.rms.oit.va.gov/SOR_Records/79VA19.asp

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?

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	This system does not collect information directly from the veteran; therefore, it does not provide privacy notices.		
Family Relation (spouse, children, parents, grandparents, etc)	N/A			
Service Information	N/A			
Medical Information	Electronic/File Transfer	This system does not collect information directly from the veteran; therefore, it does not provide privacy notices.		
Criminal Record Information	N/A			
Guardian Information	N/A			
Education Information	N/A			
Benefit Information	N/A			
Other (Explain)	Electronic/File Transfer	This system does not collect information directly from the veteran; therefore, it does not provide privacy notices.		
Some records will contain the VA purchasing agent name, credit card # and credit card expiration date. This is used for vendor billing purposes.				

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	EDP files
Family Relation (spouse, children, parents, grandparents, etc)	No			
Service Information	No			
Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory	EDP files
Criminal Record Information	No			
Guardian Information	No			
Education Information	No			
Benefit Information	No			
Other - Financial Other (Explain) Other (Explain)	Yes	VA Files / Databases (Identify file)	Mandatory	EDP files

(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	AITC EDP Programmer	Yes	Physician name, patient name and the last four digits of the veteran/patient SSN; VA purchasing agent credit card number and expiration date	Both PII & PHI	VA 6500 page 65, paragraph O - encryption of sent data
Other Veteran Organization		No			
Other Federal Government Agency	DoD	Yes	Patient information contained in the order.	Both PII & PHI	That information is not released.
State Government Agency		No			
Local Government Agency		No			
Research Entity		No			
Other Project / System		No			
Other Project / System					
Other Project / System					

(FY 2010) PIA: Access to Records

Does the system gather information from another system?		Yes
Please enter the name of the system:	EDP - Eelectronic Data Purchases	
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	n/a
Is there a contingency plan in place to process information when the system is down?		Yes

(FY 2010) 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.

Answer: A connectivity agreement is created to outline the process for authorizing access.

(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: Any information required by the vendor for processing or billing the orders is collected.

How is data checked for completeness?

Answer: EDP performs the majority of the data checking; EDY simply does syntax checking.

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

Answer: Steps were taken when the data was initially entered by the purchasing agent.

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

Answer: Steps were taken when the data was initially entered by the purchasing agent.

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

Answer:

(FY 2010) PIA: Retention & Disposal

What is the data retention period?

Answer: Purchase order information is retained for seven years. Weekly full backups occur with incremental nightly backups. Tape backups are stored off site.

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

Answer: Purchase order (procurement) information

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

Answer: Tapes containing data older than seven years are recalled and destroyed.

Where are these procedures documented?

Answer: Per VA Directive 6300 "Records and Information Management" as well as the Office on Information and Technology's Records Control Schedule 005-1 dated 08/03/09; we also verified with the Office of Acquisition and Logistics liaison. Can also use VHA Handbook 1907.1 (Section 6j) and VHA Records Control Schedule 10-1 for general guidance. In relation to the purchase orders, General Record Schedule 3 can apply.

How are data retention procedures enforced?

Answer: It is scheduled.

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 2010) 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: Prior to production, a C&A with the ATO will be complete. Prior to receiving access, the user completes and signs User Access Request Form. The user acknowledges and signs he/she will abide by the Rules of Behavior. The user also must complete mandatory security and privacy awareness training. Separate Rules of Behavior will be established for the application/system administrators with privileged accounts, including application, database, and alternate system administrators.

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 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 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 type="checkbox"/> Access Control | <input checked="" type="checkbox"/> Contingency Planning | <input type="checkbox"/> Personnel Security |
| <input checked="" type="checkbox"/> Audit and Accountability | <input type="checkbox"/> Identification and Authentication | <input type="checkbox"/> Physical and Environmental Protection |
| <input type="checkbox"/> Awareness and Training | <input checked="" type="checkbox"/> Incident Response | <input type="checkbox"/> Risk Management |
| <input checked="" type="checkbox"/> Certification and Accreditation Security Assessments | | |
| <input 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 checked="" 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 type="checkbox"/> | The potential impact is moderate if the loss 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?

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 on this tab for any question in the form you want to comment on. Please indicate the question you are responding to and then add your comments.

Purchasing agents throughout the VA medical facilities access either Denver's Remote Order Entry Systems (audiology information) or IFCAP (financial information) to place orders. EDP extracts the data from VistA (Mailman) and then performs various actions on the data. EDY takes the data from EDP and translates it into ANSI X12 format for the vendors. The reverse happens when the data is inbound from the vendors.

(FY 2011) PIA: VBA Minor Applications

Explain what minor application that are associated with your installation? (Check all that apply)

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

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

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

Explain what minor application that are associated with your installation? (Check all that apply)

	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
X	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
X	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	X 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 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: Minor Applications

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

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: Final Signatures

Facility Name: Development > CDCO > AITC > OAL > VLTrader

Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	326-6217	Amy.Howe1@va.gov
Digital Signature Block			
Information Security Officer:	Charles Aponte	326-6593	Charles.Aponte2@va.gov
Digital Signature Block			
System Owner/ CIO	Judy Downing	326-6000	Judy.Downing@va.gov
Digital Signature Block			
Information Owner:	Tammy Watson	202-461-6126	Tammy.Watson@va.gov
Digital Signature Block			
Other Titles: Supervisory IT Specialist	Chris Kelly	326-6464	Chris.Kelly@va.gov
Digital Signature Block			

Date of Report: 9/1/2010
 OMB Unique Project Identifier: Not in SMART
 Project Name: Development > CDCO > AITC > OAL > VLTrader