

Welcome to the PIA for FY 2010!

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/PIA.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 an individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirectly identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

(FY 2010) PIA: System Identification

Program or System Name: REGION 1> VHA> VISN 18> Amarillo VAMC> LAN

OMB Unique System / Application / Program

Identifier (AKA: UPID #): Exhibit 300 ID: 029-00-02-00-01-1120-00

Description of System / Application / Program: *The AVAHCS Local Area Network is a Major Application and General Support System owned by Dr. James Laub, VA Office of Information and Technology that has been determined have a security categorization of High in accordance with Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems*

Facility Name: Amarillo VAMC

Title:	Name:	Phone:	Email:
Privacy Officer:	Bob Auffrey	806-355-9703 x7524	Robert.Auffrey@va.gov
Information Security Officer:	Steve Tyrer	806-355-9703 x7065	Steve.Tyrer@va.gov
Chief Information Officer:	Modesto Baca	806-355-9703 x4000	Modesto.Baca@va.gov
Person Completing Document:	Deborah Heald	806-355-9703 x7190	Deborah.Heald@va.gov
Telecommunications Manager:	David Bressler	806-355-9703 x1531	David.Bressler@va.gov
Second Information Security Officer:	Deborah Heald	806-355-9703 x7190	Deborah.Heald@va.gov
System Owner:	Dr. James Laub	480-325-3131	James.Laub@va.gov
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	07/2009		
Date Approval To Operate Expires:	07/2011		

What specific legal authorities authorize this program or system: Title 38, United States Code, section 7301(a).

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

125,000

Identify what stage the System / Application / Program is at:

Operations/Maintenance

The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.

12 years

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): 08/2010

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 skip to TAB 12. (See Comment for Definition of PII)

(FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?

Yes

if the answer above is no, please skip to row 16.

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

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

79VA19

2. Name of the System of Records:

Vista 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?

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 2010) 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)	ALL	Health Care & Research, if approved	Verbal & Written	Verbal & Written
Family Relation (spouse, children, parents, grandparents, etc)	N/A			
Service Information	Paper	Health Care Benefits	Verbal & Written	Verbal & Written
Medical Information	Paper & Electronic	Medical Treatment	Verbal & Written	Verbal & Written
Criminal Record Information	Electronic/File Transfer	Medical Treatment	Verbal & Written	Verbal & Written
Guardian Information	N/A			
Education Information	Verbal		Verbal & Written	Verbal & Written
Benefit Information	Paper & Electronic	Health Care Benefits	Verbal & Written	Verbal & 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	Veteran	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	
Service Information	Yes	Veteran	Mandatory	
Medical Information	Yes	Veteran	Mandatory	
Criminal Record Information	Yes	Veteran	Mandatory	
Guardian Information	No		Mandatory	
Education Information	Yes	Veteran	Voluntary	
Benefit Information	Yes	Veteran	Mandatory	
Other (Explain)				
Other (Explain)				
Other (Explain)				

(FY 2010) 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	VBA, NCA,	Yes	C&P information is shared	Both PII & PHI	HINQ
Other Veteran Organization		No			
Other Federal Government Agency	CDC	No	Name; DOB; SSN; Health Info		Release of Information MCM 136-02-0609
State Government Agency	Texas State Veterans Home	No	Name; DOB; SSN; Health Info		Release of Informaiton MCM 136-02-0609
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: VistA

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 2010) PIA: Secondary Use

Will PII data be included with any secondary use request? No

if yes, please check all that apply:
 Drug/Alcohol Counseling Mental Health
 Research Sickle Cell Other (Please Explain)

Describe process for authorizing access
to this data.

Answer:

(FY 2010) 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: LAN is used to store information related to organization duties

How is data checked for completeness?

Answer: Compared to VistA data when appropriate

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

Answer: Data is kept current by daily use.

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

Answer: Through comparison with VistA and other information systems

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: Depending upon the information type as specified by NARA

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

Answer:

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

Answer: Data is marked for deletion by the operating system. Backup tapes are destroyed by a National VA contractor

Where are these procedures documented?

Answer: IT Contingency Plan

How are data retention procedures enforced?

Answer: Through daily backup of all data stored on the LAN

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 2010) 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: C&A completed 2008 and annual FISMA security control reviews.

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

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

Answer: (Other Risks)

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

- Risk Management
- Access Control
- Awareness and Training
- Contingency Planning
- Physical and Environmental Protection
- Personnel Security
- Certification and Accreditation Security Assessments
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- 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: The facility utilizes "NetIQ" to monitor the local network, analyzing system performance logs in real time while looking for availability problems to include active attacks and system and network slowdowns and "crashes". The implementation of the new Service Line Model throughout Region I has also helped our security stand in this area through the use of Region I wide system monitoring scans that are performed on a weekly and/or monthly basis.

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

(Choose One)

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

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

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

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

(Choose One)

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

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

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

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

(Choose One)

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

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

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

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 2010) 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.

(FY 2010) PIA: VBA Minor Applications

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

Records Locator System Veterans Assistance Discharge System (VADS)	Education Training Website	Appraisal System Web Electronic Lender Identification
LGY Processing	VR&E Training Website VA Reserve Educational Assistance Program	CONDO PUD Builder Centralized Property Tracking System
Loan Service and Claims LGY Home Loans	Web Automated Verification of Enrollment Right Now Web VA Online Certification of Enrollment (VA-ONCE)	Electronic Appraisal System Web LGY
Search Participant Profile (SPP)	Automated Folder Processing System (AFPS)	Access Manager
Control of Veterans Records (COVERS)	Personal Computer Generated Letters (PCGL)	SAHSHA
SHARE Modern Awards Process Development (MAP-D) Rating Board Automation 2000 (RBA2000)	Personnel Information Exchange System (PIES) Rating Board Automation 2000 (RBA2000)	VBA Data Warehouse Distribution of Operational Resources (DOOR)
State of Case/Supplemental (SOC/SSOC)	SHARE	Enterprise Wireless Messaging System (Blackberry) VBA Enterprise Messaging System
Awards	State Benefits Reference System Training and Performance Support System (TPSS)	LGY Centralized Fax System
Financial and Accounting System (FAS)	Veterans Appeals Control and Locator System (VACOLS) Veterans On-Line Applications (VONAPP)	Review of Quality (ROQ) Automated Sales Reporting (ASR)
Eligibility Verification Report (EVR) Automated Medical Information System (AMIS)290	Automated Medical Information Exchange II (AIME II)	Electronic Card System (ECS)
Web Automated Reference Material System (WARMS)	Committee on Waivers and Compromises (COWC)	Electronic Payroll Deduction (EPD)
Automated Standardized Performance Elements Nationwide (ASPEN)	Common Security User Manager (CSUM)	Financial Management Information System (FMI)
Inquiry Routing Information System (IRIS)	Compensation and Pension (C&P) Record Interchange (CAPRI) Control of Veterans Records (COVERS)	Purchase Order Management System (POMS)
National Silent Monitoring (NSM) Web Service Medical Records (WebSMR)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)	Veterans Canteen Web
Systematic Technical Accuracy Review (STAR)	Fiduciary Beneficiary System (FBS) Hearing Officer Letters and Reports System (HOLAR)	Inventory Management System (IMS)
Fiduciary STAR Case Review Veterans Exam Request Info System (VERIS) Web Automated Folder Processing System (WAFPS)	Inforce	Synquest RAI/MDS ASSISTS
Courseware Delivery System (CDS) Electronic Performance Support System (EPSS) Veterans Service Representative (VSR) Advisor	Awards Actuarial Insurance Self Service	MUSE Bbraun (CP Hemo) VIC
Loan Guaranty Training Website	Insurance Unclaimed Liabilities	BCMA Contingency Machines
C&P Training Website	Insurance Online	Script Pro

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.

Minor app #1	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?			

Minor app #2	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?			

Minor app #3	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?			

Baker System	Veterans Assistance Discharge System (VADS)
Dental Records Manager	VBA Training Academy
Sidexis	Veterans Service Network (VETSNET) Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
Priv Plus Mental Health Assistant	BIRLS
Telecare Record Manager	Centralized Accounts Receivable System (CARS)
Omnicell	Compensation & Pension (C&P)
Powerscribe Dictation System	Corporate Database
EndoSoft	Control of Veterans Records (COVERS)
Compensation and Pension (C&P)	Data Warehouse
Montgomery GI Bill Vocational Rehabilitation & Employment (VR&E) CH 31 Post Vietnam Era educational Program (VEAP) CH 32	INS - BIRLS Mobilization Master Veterans Record (MVR)
Spinal Bifida Program Ch 18	BDN Payment History
C&P Payment System	
Survivors and Dependents Education Assistance CH 35	
Reinstatement Entitlement Program for Survivors (REAPS) Educational Assistance for Members of the Selected Reserve Program CH 1606	
Reserve Educational Assistance Program CH 1607 Compensation & Pension Training Website	
Web-Enabled Approval Management System (WEAMS)	
FOCAS Work Study Management System (WSMS)	
Benefits Delivery Network (BDN) Personnel and Accounting Integrated Data and Fee Basis (PAID) Personnel Information Exchange System (PIES) Rating Board Automation 2000 (RBA2000)	
SHARE Service Member Records Tracking System	

(FY 2010) PIA: VISTA Minor Applications

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

ACCOUNTS RECEIVABLE	DRUG ACCOUNTABILITY	INPATIENT MEDICATIONS
ADP PLANNING (PLANMAN)	DSS EXTRACTS	INTAKE/OUTPUT
ADVERSE REACTION TRACKING	EDUCATION TRACKING	INTEGRATED BILLING
ASISTS	EEO COMPLAINT TRACKING	INTEGRATED PATIENT FUNDS
AUTHORIZATION/SUBSCRIPTION	ELECTRONIC SIGNATURE	INTERIM MANAGEMENT SUPPORT
AUTO REPLENISHMENT/WARD STOCK	ENGINEERING	KERNEL
AUTOMATED INFO COLLECTION SYS	ENROLLMENT APPLICATION SYSTEM	KIDS
AUTOMATED LAB INSTRUMENTS	EQUIPMENT/TURN-IN REQUEST	LAB SERVICE
AUTOMATED MED INFO EXCHANGE	EVENT CAPTURE	LETTERMAN
BAR CODE MED ADMIN	EVENT DRIVEN REPORTING	LEXICON UTILITY
BED CONTROL	EXTENSIBLE EDITOR	LIBRARY
BENEFICIARY TRAVEL	EXTERNAL PEER REVIEW	LIST MANAGER
CAPACITY MANAGEMENT - RUM	FEE BASIS	MAILMAN
CAPRI	FUNCTIONAL INDEPENDENCE	MASTER PATIENT INDEX VISTA
CAPACITY MANAGEMENT TOOLS	GEN. MED. REC. - GENERATOR	MCCR NATIONAL DATABASE
CARE MANAGEMENT	GEN. MED. REC. - I/O	MEDICINE
CLINICAL CASE REGISTRIES	GEN. MED. REC. - VITALS	MENTAL HEALTH
CLINICAL INFO RESOURCE NETWORK	GENERIC CODE SHEET	MICOM
CLINICAL MONITORING SYSTEM	GRECC	MINIMAL PATIENT DATASET
CLINICAL PROCEDURES	HEALTH DATA & INFORMATICS	MYHEALTHVET
CLINICAL REMINDERS	HEALTH LEVEL SEVEN	Missing Patient Reg (Original)
CMOP	HEALTH SUMMARY	A4EL NATIONAL DRUG FILE
CONSULT/REQUEST TRACKING	HINQ	NATIONAL LABORATORY TEST
CONTROLLED SUBSTANCES	HOSPITAL BASED HOME CARE	NDBI
CPT/HCPCS CODES	ICR - IMMUNOLOGY CASE REGISTRY	NETWORK HEALTH EXCHANGE
CREDENTIALS TRACKING	IFCAP	NOIS
DENTAL	IMAGING	NURSING SERVICE
DIETETICS	INCIDENT REPORTING	OCCURRENCE SCREEN
DISCHARGE SUMMARY	INCOME VERIFICATION MATCH	ONCOLOGY
DRG GROUPER	INCOMPLETE RECORDS TRACKING	ORDER ENTRY/RESULTS REPORTING

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.

Minor app #1	Name		Description		Comments
		<input type="checkbox"/>	Is PII collected by this min or application?		
		<input type="checkbox"/>	Does this minor application store PII?		
			If yes, where?		
		Who has access to this data?			

Minor app #2	Name		Description		Comments
		<input type="checkbox"/>	Is PII collected by this min or application?		
		<input type="checkbox"/>	Does this minor application store PII?		
			If yes, where?		
		Who has access to this data?			

Minor app #3	Name		Description		Comments
		<input type="checkbox"/>	Is PII collected by this min or application?		
		<input type="checkbox"/>	Does this minor application store PII?		
			If yes, where?		
		Who has access to this data?			

OUTPATIENT PHARMACY	SOCIAL WORK
PAID	SPINAL CORD DYSFUNCTION
PATCH MODULE	SURGERY
PATIENT DATA EXCHANGE	SURVEY GENERATOR
PATIENT FEEDBACK	TEXT INTEGRATION UTILITIES
PATIENT REPRESENTATIVE	TOOLKIT
PCE PATIENT CARE	UNWINDER
ENCOUNTER	UTILIZATION MANAGEMENT ROLLUP
PCE PATIENT/IHS SUBSET	
PHARMACY BENEFITS	UTILIZATION REVIEW
MANAGEMENT	
PHARMACY DATA	VA CERTIFIED COMPONENTS - DSSI
MANAGEMENT	
PHARMACY NATIONAL	VA FILEMAN
DATABASE	
PHARMACY PRESCRIPTION	VBECs
PRACTICE	
POLICE & SECURITY	VDEF
PROBLEM LIST	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES	VHS&RA ADP TRACKING SYSTEM
PROSTHETICS	VISIT TRACKING
QUALITY ASSURANCE	VISTALINK
INTEGRATION	
QUALITY IMPROVEMENT	VISTALINK SECURITY
CHECKLIST	
QUASAR	VISUAL IMPAIRMENT SERVICE TEAM
	ANRV
RADIOLOGY/NUCLEAR	VOLUNTARY TIMEKEEPING
MEDICINE	
RECORD TRACKING	VOLUNTARY TIMEKEEPING NATIONAL
REGISTRATION	WOMEN'S HEALTH
RELEASE OF INFORMATION - DSSI	CARE TRACKER
REMOTE ORDER/ENTRY	
SYSTEM	
RPC BROKER	
RUN TIME LIBRARY	
SAGG	
SCHEDULING	
SECURITY SUITE UTILITY PACK	
SHIFT CHANGE HANDOFF	
TOOL	

(FY 2010) 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
Minor app #1	<input type="checkbox"/> Is PII collected by this min or application?	
	<input type="checkbox"/> Does this minor application store PII?	
	If yes, where?	
	Who has access to this data?	

Name	Description	Comments
Minor app #2	<input type="checkbox"/> Is PII collected by this min or application?	
	<input type="checkbox"/> Does this minor application store PII?	
	If yes, where?	
	Who has access to this data?	

Name	Description	Comments
Minor app #3	<input type="checkbox"/> Is PII collected by this min or application?	
	<input type="checkbox"/> Does this minor application store PII?	
	If yes, where?	
	Who has access to this data?	

(FY 2010) PIA: Final Signatures

Facility Name: Amarillo VAMC

Title:	Name:	Phone:	Email:
Privacy Officer:	Bob Auffrey	806-355-9703 x7524	Robert.Auffrey@va.gov
Information Security Officer:	Deborah Heald	806-355-9703 x7065	Deborah.Heald@va.gov
Chief Information Officer:	Modesto Baca	806-355-9703 x4000	Modesto.Baca@va.gov
Person Completing Document:	Deborah Heald	806-355-9703 x7065	Deborah.Heald@va.gov
System / Application / Program Manager:	David Bressler	806-355-9703 x1531	David.Bressler@va.gov

Date of Report: 7/29/2010

OMB Unique Project Identifier Exhibit 300 ID: 029-00-02-00-01-1120-00

Project Name REGION 1>VHA>VISN 18>Amarillo VAMC>LAN

The Signature Process:

- Complete the PIA form.
- Name the PIA Excel FORM ["FY09-Region # - Facility Name - Facility # -Date(mmddyyyy).xls"]
 - Example: "FY09-Region3-Lexington VAMC-596-10302008.xls"
- Submit the completed PIA Excel form to SMART Database.
- Fix errors the reviewers sent back, rename the file and submit to SMART Database
- If no errors, convert form into PDF with Nuance PDF Professional.
- Name the PIA PDF form ["FY09-Region #-Facility Name- Facility # -Date(mmddyyyy).xls"]
- Remove the Security Tab ****Will not be published!****
- Obtain digital signatures on the "Final Signatures tab"
- Submit signed PIA PDF form to the SMART Database.