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://vaww.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

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 indentify 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 2010) PIA: System Identification

Program or System Name:	VistA West Texas VA Health Care System (519 - Big Spring, TX)
OMB Unique System / Application / Program Identifier (AKA: UPID #):	Exhibit 300 ID: 029-00-01-11-01-1180-00
Description of System / Application / Program:	The West Texas VA Healthcare System (WTVAHCS) VistA is identified by VA OI&T as an information system that meets criteria for Certification and Accreditation activities. VistA was certified in Fiscal Year 2005 as an accredited system for use by the Veterans Administration (VA) staff in the conduct of official VA business and deemed essential for business activities. This analysis is conducted at least annually or in the event that significant changes occurs with the system.

Facility Name:	West Texas VA Healthcare System (WTVAHCS)		
Title:	Name:	Phone:	Email:
Privacy Officer:	Geneva Cox	432-263-7361	geneva.cox@va.gov
Information Security Officer:	Mike McKinley	432-268-2561	john.mckinley@va.gov
Chief Information Officer:	Greg Moore	432-268-2546	greg.moore@va.gov
Person Completing Document:	Kelly Paige	432-263-7361	kelly.paige@va.gov
System Administrator	Royce Islas	432-268-2545	royce.islas@va.gov
Other Titles:			
Other Titles:			
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	04/2008		
Date Approval To Operate Expires:	04/2010		

What specific legal authorities authorize this program or system:	79VA19 - Veterans Health Information Systems and Technology Architecture (Vista) Records - VA Title 38, United States Code, section 7301(a).
What is the expected number of individuals that will have their PII stored in this system:	100,000
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.	10 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):	03/2010

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
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?	Yes
	(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	Used for communication, benefit determination, 1st and 3rd party billing and collection, overall treatment of the Veteran	All	Verbal & Written
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Used for communication, benefit determination, 1st and 3rd party billing and collection, overall treatment of the Veteran	All	Verbal & Written
Service Information	ALL	Used for communication, benefit determination, 1st and 3rd party billing and collection, overall treatment of the Veteran	All	Verbal & Written
Medical Information	ALL	Used for communication, benefit determination, 1st and 3rd party billing and collection, overall treatment of the Veteran	All	Verbal & Written
Criminal Record Information		Information is not retained within Vista		
Guardian Information	ALL	Used for communication, benefit determination, 1st and 3rd party billing and collection, overall treatment of the Veteran	All	Verbal & Written
Education Information	ALL	Used for communication, benefit determination, 1st and 3rd party billing and collection, overall treatment of the Veteran	All	Verbal & Written
Benefit Information	ALL	Used for communication, benefit determination, 1st and 3rd party billing and collection, overall treatment of the Veteran	All	Verbal & Written
Other (Explain)		Used for communication, benefit determination, 1st and 3rd party billing and collection, overall treatment of the Veteran	All	Verbal & Written

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	Records are created to support patient care, benefits available, 1st and 3rd party billing and collection, statistical information and other reports
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Criminal Record Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Guardian Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Education Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Benefit Information	Yes	VA Files / Databases (Identify file)	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	WTVAHCS	Yes	Veteran Benefits, service dates, name, SSN to DAV, VBA, DoD and NCA	Both PII & PHI	Shared via other VA sites using Remote Data View to see information.
Other Veteran Organization		No		N/A	
Other Federal Government Agency	DoD	No	Sharing for individuals for further treatment and sharing agreement process	N/A	
State Government Agency	State Tumor Registry State Veterans Home	Yes	Tumor Registry information is shared with the State Tumor Registry for statistical purposes. State Veterans Home has read-only access for current eligibility and financial information	PHI	Information is shared by local VA staff member logging into their database and uploading statistical information.
Local Government Agency		No		N/A	
Research Entity		No		N/A	
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2010) PIA: Access to Records

Does the system gather information from another system?	No
Please enter the name of the system:	
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?	Yes
if yes, please check all that apply:	☑ Drug/Alcohol Counseling ☑ Mental Health ☐ HIV ☐ Research ☐ Sickle Cell ☐ Other (Please Explain)
Describe process for authorizing access to this data. Answer:	ROI Request

(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: Only required eliments are mandated for entry

How is data checked for completeness?

Answer: System will not allow progression unless all required fields have been completed

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

Answer: Data is verified with each visit

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

Answer: Verified verbally or in Writing

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: 75 years after last episode of care

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

Answer: The time frame is mandated by the VHA Records Control Schedule

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

Answer: Deletion or destroy records

Where are these procedures documented?

Answer: 44 U.S.C. Chapter 33

How are data retention procedures enforced?

Answer: Backups are performed on regular basis and authorization to delete records is extremely limited.

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: System was Certified and Accredited for use by VA	

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)
- ☐ Burglary/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: There have been no changes made to the VistA system; however, we have made and are still making changes in the actual use of the documents available from VistA such as the routing slip given to the patient at the time of check in and the required medication reconciliation done with the MD.

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)

- [x] 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)

- [x] 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)

- [x] 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:

Verification of the information taken from the appropriate staff for address, phone number, next of kin, insurance information, etc. Patient's MD goes over medications for reconciliation and clinic nurses review allergies, etc. at each appointment.

(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)
LGY Processing
Loan Service and Claims
LGY Home Loans
Search Participant Profile (SPP)
Control of Veterans Records (COVERS)
SHARE
Modern Awards Process Development (MAP-D)
Rating Board Automation 2000 (RBA2000)
State of Case/Supplemental (SOC/SSOC)
Awards
Financial and Accounting System (FAS)
Eligibility Verification Report (EVR)
Automated Medical Information System (AMIS)290
Web Automated Reference Material System (WARMS)
Automated Standardized Performace Elements Nationwide (ASPEN)
Inquiry Routing Information System (IRIS)
National Silent Monitoring (NSM)
Web Service Medical Records (WebSMR)
Systematic Technical Accuracy Review (STAR)
Fiduciary STAR Case Review
Veterans Exam Request Info System (VERIS)
Web Automated Folder Processing System (WAFPS)
Courseware Delivery System (CDS)
Electronic Performance Support System (EPSS)
Veterans Service Representative (VSR) Advisor
Loan Guaranty Training Website
C&P Training Website

Education Training Website
VR&E Training Website
VA Reserve Educational Assistance Program
Web Automated Verification of Enrollment
Right Now Web
VA Online Certification of Enrollment (VA-ONCE
Automated Folder Processing System (AFPS)
Personal Computer Generated Letters (PCGL)
Personnel Information Exchange System (PIES)
Rating Board Automation 2000 (RBA2000)
SHARE
State Benefits Reference System
Training and Performance Support System (TPSS)
Veterans Appeals Control and Locator System (VACOLS)
Veterans On-Line Applications (VONAPP)
Automated Medical Information Exchange II (AIME II)
Committee on Waivers and Compromises (COWC)
Common Security User Manager (CSUM)
Compensation and Pension (C&P) Record Interchange (CAPRI)
Control of Veterans Records (COVERS)
Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
Fiduciary Beneficiary System (FBS)
Hearing Officer Letters and Reports System (HOLAR)
Inforce
Awards
Actuarial
Insurance Self Service
Insurance Unclaimed Liabilities
Insurance Online

Appraisal System
Web Electronic Lender Identification
CONDO PUD Builder
Centralized Property Tracking System
Electronic Appraisal System
Web LGY
Access Manager
SAHSHA
VBA Data Warehouse
Distribution of Operational Resources (DOOR)
Enterprise Wireless Messaging System (Blackberry)
VBA Enterprise Messaging System
LGY Centralized Fax System
Review of Quality (ROQ)
Automated Sales Reporting (ASR)
Electronic Card System (ECS)
Electronic Payroll Deduction (EPD)
Financial Management Information System (FMI)
Purchase Order Management System (POMS)
Veterans Canteen Web
Inventory Management System (IMS)
Synquest
RAI/MDS
ASSISTS
MUSE
Bbraun (CP Hemo)
VIC
BCMA Contingency Machines
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.

	Name		Description		Comments

Minor app #1

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

Minor app #2

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

Minor app #3

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

Dental Records Manager

Sidexis

Priv Plus
Mental Health Asisstant

Telecare Record Manager

Omnicell

Powerscribe Dictation System

EndoSoft

Compensation and Pension (C&P)

Montgomery GI Bill
Vocational Rehabilitation & Employment (VR&E) CH 31
Post Vietnam Era educational Program (VEAP) CH 32

Spinal Bifida Program Ch 18

C&P Payment System

Survivors and Dependents Education Assistance CH 35

Reinstatement Entitelment 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

Veterans Assistance Discharge System (VADS)

VBA Training Academy

Veterans Service Network (VETSNET)
Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
BIRLS
Centralized Accounts Receivable System (CARS)

Compensation & Pension (C&P)

Corporate Database

Control of Veterans Records (COVERS)

Data Warehouse

INS - BIRLS

Mobilization

Master Veterans Record (MVR

BDN Payment History

(FY 2010) PIA: VISTA Minor Applications

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

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

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?		
Minor app #1			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?		
Minor app #2			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?		
Minor app #3			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

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

(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

	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

Minor app #2

	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

Minor app #3

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

(FY 2010) PIA: Final Signatures

Facility Name: West Texas VA Healthcare System (WTVAHCS)

Title:	Name:	Phone:	Email:
Privacy Officer:	Geneva Cox	432-263-7361	geneva.cox@va.gov
Digital Signature Block			
Information Security Officer:	Mike McKinley	432-268-2561	john.mckinley@va.gov
Digital Signature Block			
Chief Information Officer:	Greg Moore	432-268-2546	greg.moore@va.gov
Digital Signature Block			
Person Completing Document:	Kelly Paige	432-263-7361	kelly.paige@va.gov
Digital Signature Block			
System / Application / Program Manager:	Royce Islas	432-268-2545	royce.islas@va.gov
Digital Signature Block			

Date of Report: 3/5/2010

OMB Unique Project Identifier: Exhibit 300 ID: 029-00-01-11-01-1180-00

VISTA SIGNATURES

Project Name

VistA West Texas VA Health Care System (519 - Big Spring, TX)

VISTA SIGNATURES