

## **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 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 2010) PIA: System Identification

Program or System Name: Region 2, VHA, VISN 17, South Texas Veterans HCS Vista – VMS System

OMB Unique System / Application / Program Identifier (AKA: UPID #):

029-00-01-11-01-1180-00

Description of System / Application / Program:

The south Texas Veterans HCS Vista – VMS System is the software platform and hardware infrastructure (associated with clinical operations) on which software applications operate on and E-Government initiatives are supported. The south Texas Veterans HCS Vista – VMS System includes the computer equipment associated with clinical and administrative operations and the employees necessary to operate the system. The south Texas Veterans HCS Vista – VMS System is a client-server system linking the south Texas Facility computer network to over 100 applications and databases. The south Texas Veterans HCS Vista – VMS System provides critical data that supports the delivery of healthcare to veterans and their dependants. Using the computer, the VA health care providers can access Vista-Legacy applications and meet a wide range of health care data needs. The south Texas Veterans HCS Vista – VMS System encompasses a variety of clinical and administrative applications, some on single use platforms and is currently running interSystems Cache on Virtual Memory System Cache (VMS/Cache). The south Texas Veterans HCS Vista – VMS System supports a multitude of

Facility Name: South Texas Veterans Health Care System

Title:

Name:

Phone:

Email:

Privacy Officer:  
Information Security Officer:  
Chief Information Officer:

Mary L. Wohl	210 617 5300	<a href="mailto:Mary.Wohl@va.gov">Mary.Wohl@va.gov</a>
Gerald Steward	ex 15602	<a href="mailto:Gerald.Steward@va.gov">Gerald.Steward@va.gov</a>
Simon Willett	210 616 8165	<a href="mailto:Simon.willett@va.gov">Simon.willett@va.gov</a>
	210 617 5126	
	210 617 5300	
Mary L. Wohl	ex 15602	<a href="mailto:Mary.Wohl@va.gov">Mary.Wohl@va.gov</a>

Person Completing Document:

Other Titles:

Other Titles:

Date of Last PIA Approved by VACO

Privacy Services: (MM/YYYY)

Date Approval To Operate Expires:

03/2009

01/2011

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.

20+

Is there an authorized change control process which documents any changes to existing applications or systems?

No

If No, please explain:

All changes are recorded and ran through testing to ensure capability and control All changes are monitored by the Systems Manager/Owner

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?

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

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: VistA-VMS
3. Location where the specific applicable System of Records Notice may be accessed (include the URL): <http://vaww.vacho.va.gov/privacy/System of Records.htm>

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

Yes

Does the System of Records Notice require modification or updating?

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.

<b>Data Type</b>	<b>Collection Method</b>	<b>What will the subjects be told about the information collection?</b>	<b>How is this message conveyed to them?</b>	<b>How is a privacy notice provided?</b>
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Verbal	Veteran	Verbally	Written
Family Relation (spouse, children, parents, grandparents, etc)	Verbal	Veteran	Written	Written
Service Information	Electronic/File Transfer	Veteran	Written	Written
Medical Information	Electronic/File Transfer	Veteran	Written	Written
Criminal Record Information	Electronic/File Transfer	Veteran	Written	Written
Guardian Information				
Education Information				
Benefit Information				
Other (Explain)				

<b>Data Type</b>	<b>Is Data Type Stored on your system?</b>	<b>Source</b> (If requested, identify the specific file, entity and/or name of agency)	<b>Is data collection Mandatory or Voluntary?</b>	<b>Additional Comments</b>
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Mandatory	
Service Information	Yes	Veteran	Mandatory	
Medical Information	Yes	Veteran	Mandatory	
Criminal Record Information	Yes	Veteran	Mandatory	
Guardian Information	Yes	Veteran	Mandatory	
Education Information	Yes	Veteran	Voluntary	
Benefit Information	Yes	Veteran	Mandatory	
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	VARO/NBA	Yes	benefits and medical exc	Both PII & PHI	Release of Information
Other Veteran Organization	VSO	No	medical information	Both PII & PHI	Release of Information
Other Federal Government Agency					
State Government Agency					
Local Government Agency					
Research Entity					
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?

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  
 Research  
 Sickle Cell  
 Other (Please Explain)  
 Mental Health  
 HIV

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?

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: Only required elements are entered into the system.

How is data checked for completeness?

Answer: Random audits/inconsistency reports. Staff also reviews data.

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

Answer: Update/review for each appointment also preregistration

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

Answer: Health Enrollment Center staff reviews data for accuracy.

*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?

75 yrs

Answer: Clinical information is retained in accordance with VA Records Control Schedule 10-1. Demographic information is updated as applications for care are submitted and retained in accordance with VA Records Control Schedule 10-1. The information is retained for the periods specified in the schedule because it is the main authority for the retention & disposition requirements.

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

Answer: Duration span of life

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

Answer: Electronic Final Version of Patient Medical Record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records Control Schedule 10-1, Item XLIII, 2.b. (Page 190). At the present time, Vista Imaging retains all images.

Where are these procedures documented?

Answer: VA Handbook 6300; Record Control Schedule 10-1

How are data retention procedures enforced?

Answer: VA Records Control Schedule 10-1 (page 8): Records Management Responsibilities The Health Information Resources Service (HIRS) is responsible for developing policies and procedures for effective and efficient records management throughout VHA. In addition, HIRS acts as the liaison between VHA and National Archives and Records Administration (NARA) on issues pertaining to records management practices and procedures. Field records officers are responsible for records management activities at their facilities. Program officials are responsible for creating, maintaining, protecting, and disposing of records in their program area in accordance with NARA regulations and VA policy. All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures. These standards are enforced by VHA and field facilities.

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,

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: In order to meet all the requirements listed above, following VA National Policies, OMB policies, FISMA, and NIST guidelines, ensures this system meets or exceeds the IT security requirements of federal law, local North Texas Healthcare System policy and procedures have been put in place.

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

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

Answer: (Other Risks)

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

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

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: Unnecessary collection of information is being reduced twice a week when/wherever possible.

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

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

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

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

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

x	ACCOUNTS RECEIVABLE	x	DRUG ACCOUNTABILITY	x	INPATIENT MEDICATIONS	x	OUTPATIENT PHARMACY	x	SOCIAL WORK
x	ADP PLANNING (PLANMAN)	x	DSS EXTRACTS	x	INTAKE/OUTPUT	x	PAID	x	SOCIAL WORK
x	ADVERSE REACTION TRACKING	x	EDUCATION TRACKING	x	INTEGRATED BILLING	x	PATCH MODULE	x	SPINAL CORD DYSFUNCTION SURGERY
x	ASISTS	x	EEO COMPLAINT TRACKING	x	INTEGRATED PATIENT FUNDS	x	PATIENT DATA EXCHANGE	x	SURVEY GENERATOR
	AUTHORIZATION/SUBSCRIPTION	x	ELECTRONIC SIGNATURE		INTERIM MANAGEMENT		PATIENT FEEDBACK	x	TEXT INTEGRATION UTILITIES
x	AUTO REPLENISHMENT/WARD STOCK	x	ENGINEERING	x	SUPPORT KERNEL	x	PATIENT REPRESENTATIVE	x	TOOLKIT
x	AUTOMATED INFO COLLECTION SYS	x	ENROLLMENT APPLICATION SYSTEM		KIDS	x	PCE PATIENT CARE ENCOUNTER		UNWINDER
	AUTOMATED LAB INSTRUMENTS	x	EQUIPMENT/TURN-IN REQUEST	x	LAB SERVICE	x	PCE PATIENT/IHS SUBSET		UTILIZATION MANAGEMENT ROLLUP
x	AUTOMATED MED INFO EXCHANGE	x	EVENT CAPTURE		LETTERMAN		PHARMACY BENEFITS	x	UTILIZATION REVIEW
x	BAR CODE MED ADMIN		EVENT DRIVEN REPORTING	x	LEXICON UTILITY	x	PHARMACY DATA MANAGEMENT		VA CERTIFIED COMPONENTS - DSSI
	BED CONTROL		EXTENSIBLE EDITOR		LIBRARY	x	PHARMACY NATIONAL DATABASE	x	VA FILEMAN
x	BENEFICIARY TRAVEL		EXTERNAL PEER REVIEW	x	LIST MANAGER	x	PHARMACY PRESCRIPTION PRACTICE		VBECS
	CAPACITY MANAGEMENT - RUM	x	FEE BASIS	x	MALIMAN		POLICE & SECURITY	x	VDEF
x	CAPRI		FUNCTIONAL INDEPENDENCE	x	MASTER PATIENT INDEX		PROBLEM LIST		VENDOR - DOCUMENT STORAGE SYS
x	CAPACITY MANAGEMENT TOOLS		GEN. MED. REC. - GENERATOR	x	VISTA		PROGRESS NOTES		VHS&RA ADP TRACKING SYSTEM
x	CARE MANAGEMENT		GEN. MED. REC. - I/O	x	MCCR NATIONAL DATABASE	x	PROSTHETICS	x	VISIT TRACKING
x	CLINICAL CASE REGISTRIES	x	GEN. MED. REC. - VITALS	x	MEDICINE	x	QUALITY ASSURANCE INTEGRATION		VISITLINK
	CLINICAL INFO RESOURCE NETWORK	x	GENERIC CODE SHEET		MENTAL HEALTH		QUALITY IMPROVEMENT CHECKLIST		VISITLINK SECURITY
	CLINICAL MONITORING SYSTEM		GRECC	x	MICOM		QUASAR	x	VISUAL IMPAIRMENT SERVICE TEAM
	CLINICAL PROCEDURES	x	HEALTH DATA & INFORMATICS	x	MINIMAL PATIENT DATASET	x	RADIOLOGY/NUCLEAR MEDICINE		ANRV
x	CLINICAL REMINDERS	x	HEALTH LEVEL SEVEN		MYHEALTHVET	x	RECORD TRACKING		VOLUNTARY TIMEKEEPING
x	CMOP	x	HEALTH SUMMARY	x	Missing Patient Reg (Original)	x	REGISTRATION		VOLUNTARY TIMEKEEPING NATIONAL
x	CONSULT/REQUEST TRACKING	x	HINQ		AAEL		RELEASE OF INFORMATION - DSSI		WOMEN'S HEALTH
x	CONTROLLED SUBSTANCES	x	HOSPITAL BASED HOME CARE		NATIONAL LABORATORY TEST	x	REMOTE ORDER/ENTRY SYSTEM		CARE TRACKER
x	CPT/HPCS CODES	x	ICR - IMMUNOLOGY CASE REGISTRY		NDBI	x	RPC BROKER		
x	CREDENTIALS TRACKING	x	JFCAP	x	NETWORK HEALTH EXCHANGE		RUN TIME LIBRARY		
x	DENTAL DIETETICS	x	IMAGING INCIDENT REPORTING	x	NOIS	x	SAGG		
x	DISCHARGE SUMMARY	x	INCOME VERIFICATION MATCH	x	NURSING SERVICE OCCURRENCE SCREEN	x	SCHEDULELING		
x	DRG GROUPER	x	INCOMPLETE RECORDS TRACKING	x	ONCOLOGY	x	SECURITY SUITE UTILITY PACK		
					ORDER ENTRY/RESULTS REPORTING	x	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.

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?		

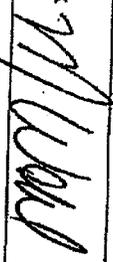
Minor app #3	Name		Description	Comments
			Is PII collected by this min or application?	
			Does this minor application store PII?	
			If yes, where?	
		Who has access to this data?		

(FY 2010) PIA: Final Signatures

Facility Name: South Texas Veterans Health Care System

Title: Name: Phone: Email:

Privacy Officer: Mary L Wohl 210 617 5300 ex 15602 Mary.Wohl@va.gov

Digital Signature Block  


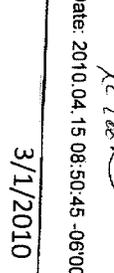
Information Security Officer: Gerald Steward 210 616 8165 Gerald.Steward@va.gov

Digital Signature Block  


Chief Information Officer: Simon Willett 210 617 5126 simon.willett@va.gov

Digital Signature Block  


Person Completing Document: Mary L Wohl 210 617 5300 ex 15602 Mary.Wohl@va.gov

Digital Signature Block  


System / Application / Program Manager: 0 0

Digital Signature Block  
Date: 2010.04.15 08:50:45 -0600  


Date of Report: 3/1/2010  
OMB Unique Project Identifier: 029-00-01-11-01-1180-00  
Project Name: Region 2, VHA, V17, STXVHCS Vista - VMS System