

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> STVHCS> LAN

OMB Unique System / Application / Program Identifier

(AKA: UPID #):

029-00-02-00-01-1120-00

Description of System / Application / Program:

The South Texas Veterans HCS LAN is the hardware infrastructure on which software applications operate on and E-Government initiatives are supported, also known as a General Support System. The South Texas Veterans HCS LAN supports mission-critical and other systems necessary to conduct day-to-day operations within the Veteran Health Administration. Applications and devices within the South Texas Veterans HCS LAN support numerous areas including medical imaging supply management, decision support, medical research, and education. It includes the computer equipment associated with clinical operations and the employees necessary to operate the system. The South Texas Veterans HCS LAN is fully operational and provides infrastructure to VA information systems, supporting IT services across the South Texas Region to include our Outpatient Clinics (Frank

Facility Name:

South Texas Veterans Health Care System

Title:

Name:

Phone:

Email:

Privacy Officer:

Mary L. Wohl

210 617 5300

Mary.Wohl@va.gov

Information Security Officer:

Gerald Steward

210 616 8165

Gerald.Steward@va.gov

Chief Information Officer:

Simon Willett

210 617 5126

simon.willett@va.gov

Person Completing Document:

Mary L. Wohl

210 617 5300

Mary.Wohl@va.gov

Other Titles:

Other Titles:

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

03/2009

Date Approval To Operate Expires:

01/2011

What specific legal authorities authorize this program or system:

Title 38, USC Section 7301 (a)

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

300,000

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.

20+

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

If No, please explain:

No

Has a PIA been completed within the last three years?

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

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, Tempe, LMS, Financial Support Systems,
Employee Support System, Medical devices,
Remedy Incident Report System, Privacy
Violation Tracking System
http://vaww.va.cha.va.gov/privacy/system_of_records.htm

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

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: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PI or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VARO/VBA	Yes	benefits and medical exc	Both PI & PHI	Release of information
Other Veteran Organization	VSO	Yes	medical information	Both PI & PHI	Release of information
Other Federal Government Agency		No			
State Government Agency		No			
Local Government Agency		No			
Research Entity		No			
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2010) PIA: Access to Records

Does the system gather information from another system? No

Please enter the name of the system: N/A

Per responses in Tab 4, does the system gather information from an individual? No

If information is gathered from an individual, is the information provided: 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 HIV 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?

If Yes, Please Specify:

No

Explain how collected data are limited to required elements. Answer: Data is e-collected as required based on the automation of VA forms and clinical procedures.

How is data checked for completeness?

Answer: Data is reviewed by staff.

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

Answer: Data is reviewed and updated as required.

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

Answer: 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?

Answer: Information is retained in accordance with VA Records Control Schedule 10-1.

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

Answer: HIPAA privacy rules covers/require retention of health information as well.

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

Answer: Contained in VA handbook/policies that address sanitization/disposal of VA data.

Where are these procedures documented?

Answer: VA directives/handbooks 1907.1/6300.1/6500. Also NIST guidance.

How are data retention procedures enforced?

Answer: Through audit and monitoring to ensure staff is complying with VA policies/regulations

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

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

Answer:

(FY 2010) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?

If Yes, How will parental or guardian approval be obtained?

Answer: No

(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: Yes

Is adequate physical security in place to protect against unauthorized access?

Yes

If 'No' please describe why:

Answer: Yes
Explain how the project meets IT security requirements and procedures required by Federal law.

System Security Plan. All security controls are implemented through a cohesive security structure and is geared to mitigating risk to information and information resources to acceptable levels. In addition to risk management, other management level controls such as system security planning, certification and accreditation and security reviews are also implemented to assure that controls reflect management policies at operational levels including at the enterprise, business line and project level. Operational and technical controls such as contingency planning input/output setting, data integrity and validation measures and logical access control) are implemented on the various network's system, server and application levels to assure that information is secured in transit. Process and storage. For example, the VA employs a virtual private network to assure the privacy of information in transit. This system works in conjunction with strong authentication measures to ensure and authenticate the identification of VA network users. System interconnection agreement (SIAs) are a system level measure to ensure that all interconnected systems meet minimum VA access policies for interconnected systems from within

Answer:

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
- Continuity 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: 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 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	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 Training and Performance Support System (TPSS)	VBA Enterprise Messaging System
Financial and Accounting System (FAS)	Veterans Appeals Control and Locator System (VACOLS)	LGY Centralized Fax System
Eligibility Verification Report (EVR)	Veterans On-Line Applications (VONAPP)	Review of Quality (ROQ)
Automated Medical Information System (AMIS)290	Automated Medical Information Exchange II (AIME II)	Automated Sales Reporting (ASR)
Web Automated Reference Material System (WARMS)	Committee on Waivers and Compromises (COWC)	Electronic Card System (ECS)
Automated Standardized Performance Elements Nationwide (ASPEN)	Common Security User Manager (CSUM)	Electronic Payroll Deduction (EPD)
Inquiry Routing Information System (IRIS)	Compensation and Pension (C&P) Record Interchange (CAPRI)	Financial Management Information System (FMI)
National Silent Monitoring (NSM)	Control of Veterans Records (COVERS)	Purchase Order Management System (POMS)
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)	Inventory Management System (IMS)
Fiduciary STAR Case Review	Hearing Officer Letters and Reports System (HOLAR)	Synquest
Veterans Exam Request Info System (VERIS)	Inforce	RAI/MDS
Web Automated Folder Processing System (WAFPS)	Awards	ASSISTS
Courseware Delivery System (CDS)	Actuarial	MUSE
Electronic Performance Support System (EPSS)	Insurance Self Service	Bbraun (CP Hemo)
Veterans Service Representative (VSR) Advisor	Insurance Unclaimed Liabilities	VIC
Loan Guaranty Training Website	Insurance Online	BCMA Contingency Machines
C&P Training Website		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
<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 #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

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

(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:

Title:

South Texas Veterans Health Care System

Name:

Phone:

Email:

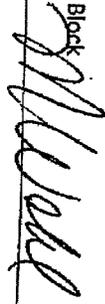
Privacy Officer:

Mary L Wohl

210 617 5300 ex 15602

Mary.Wohl@va.gov

Digital Signature Block



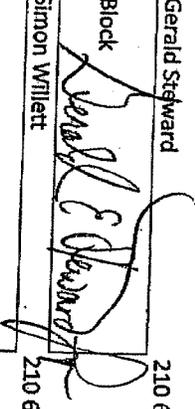
Information Security Officer:

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:

Digital Signature Block



Date: 2010.04.15 08:48:37 -06'00'

Date of Report:

3/1/2010

OMB Unique Project Identifier

029-00-02-00-01-1120-00

Project Name

Region 2> VHA> VISN 17>
STVHCS> LAN