

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

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.

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.

Identification

Program or System Name: [REGION 1 > VHA > VISN 22 > Greater Los Angeles
HCS \(West LA\) > VistA-VMS](#)

OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-01-11-01-1180-00

The VistA System is the primary application that supports VA Greater Los Angeles Healthcare System users in their day-to-day operations. This information system is continuously used during business and non-business hours, supporting many businesses processing within the agency's computing environment. The confidentiality, integrity and availability of the VistA system is critical, i.e., ensuring that data is only received by the persons and applications that it is intended for, that data is not subject to unauthorized or accidental alterations, and that the resources are available when needed. Due to the sensitivity of this information system, all personnel with system administration rights and roles will required an elevated background investigation to fulfill their

Description of System / Application / Program: duties.

Facility Name: VA Greater Los Angeles Healthcare System

Title:	Name:	Phone:
Privacy Officer:	Jenelle Happy	(818) 478-3711
Information Security Officer:	Dewitt Sanders	(818) 891-7711
Chief Information Officer:	Eugene Archey	(818) 895-9448
Person Completing Document:	Dewitt Sanders	(818) 891-7711
Other Titles:		

Other Titles:

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY) 08/2008
Date Approval To Operate Expires: 08/2011

What specific legal authorities authorize this program or system: Title 38, United States Code, section 7301(a); 501(b) and Section 304.

What is the expected number of individuals that will have their PII stored in this system: 260,000

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. 1984

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?

- 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)

Email:

jenelda.happy@va.gov

dewitt.sanders@va.gov

eugene.archey@va.gov

dewitt.sanders@va.gov

r others performing work
tifier, symbol, or othe

tifier, symbol, or othe

(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, 24VA19

2. Name of the System of Records:

VistA-VA; Patient Medical Records

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

<http://vawww.vhaco.va.gov/privacy/SystemofRecords.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?

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)	Paper & Electronic	Collection is for treatment, payment, healthcare operations, and VA Benefits; Notice of Privacy Practices; Federal Register Public Notice of Routine Uses, Storage, Retrievability, Safeguards, Retention and Disposal, Notification period, System Managers and Address, Notification, Access and Contesting Procedure, Record Source Categories.	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	Paper & Electronic	healthcare operations, and VA Benefits; Notice of Privacy Practices; Federal	Written	Written
Service Information	Paper & Electronic	Collection is for treatment, payment, healthcare operations, and VA Benefits; Notice of Privacy Practices; Federal Register Public Notice of Routine Uses, Storage, Retrievability, Safeguards, Retention and Disposal, Notification period, System Managers and Address, Notification, Access and Contesting Procedure, Record Source Categories.	Written	Written
Medical Information	Paper & Electronic	Collection is for treatment, payment, healthcare operations, and VA Benefits; Notice of Privacy Practices; Federal Register Public Notice of Routine Uses, Storage, Retrievability, Safeguards, Retention and Disposal, Notification period, System Managers and Address, Notification, Access and Contesting Procedure, Record Source Categories.	Written	Written

Criminal Record Information	ALL	Collection is for treatment, payment, healthcare operations, and VA Benefits; Notice of Privacy Practices; Federal Register Public Notice of Routine Uses, Storage, Retrievability, Safeguards, Retention and Disposal, Notification period, System Managers and Address, Notification, Access and Contesting Procedure, Record Source Categories.	Written	Written
Guardian Information	Paper & Electronic	Collection is for treatment, payment, healthcare operations, and VA Benefits; Notice of Privacy Practices; Federal Register Public Notice of Routine Uses, Storage, Retrievability, Safeguards, Retention and Disposal, Notification period, System Managers and Address, Notification, Access and Contesting Procedure, Record Source Categories.	Written	Written
Education Information	Paper & Electronic	Collection is for treatment, payment, healthcare operations, and VA Benefits; Notice of Privacy Practices; Federal Register Public Notice of Routine Uses, Storage, Retrievability, Safeguards, Retention and Disposal, Notification period, System Managers and Address, Notification, Access and Contesting Procedure, Record Source Categories.	Written	Written
Benefit Information	Paper & Electronic	Collection is for treatment, payment, healthcare operations, and VA Benefits; Notice of Privacy Practices; Federal Register Public Notice of Routine Uses, Storage, Retrievability, Safeguards, Retention and Disposal, Notification period, System Managers and Address, Notification, Access and Contesting Procedure, Record Source Categories.	Written	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	Written
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	Written
Service Information	Yes	Other Federal Agency (Identify)	Mandatory	Written
Medical Information	Yes	Veteran	Mandatory	Written
Criminal Record Information	No			
Guardian Information	Yes	Veteran	Mandatory	Written
Education Information	Yes	Veteran	Voluntary	Written
Benefit Information	Yes	Other Federal Agency (Identify)	Mandatory	Written
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	VHA; VBA; NCA; OIG; OGC; HRC	Yes	Treatment, payment, benefits, and healthcare operations; Legal Representation; Law Enforcement; Adjudication of Claims; VA Benefits	Both PII & PHI	VHA Handbook 1605.1; Standing Letter Agreements
Other Veteran Organization	VSO	Yes	Medical and Benefit and Healthcare information for veteran benefit assistance	N/A	VHA Handbook 1605.1; Patient Authorization
Other Federal Government Agency	VHA; VBA; SSA; DOD; DOJ; FDA	Yes	Treatment, payment, benefits, and healthcare operations	Both PII & PHI	VHA Handbook 1605.1; .1: Sharing Agreements; Business Associate Agreements; Standing Letters; Health and Safety
State Government Agency	State of California, California Department of Public Health; Medical Board of California; California State Veteran Homes; Organ Procurement Organization	No	Health and Safety; Criminal Activity: Donor Purposes	Both PII & PHI	VHA Handbook 1605.1; Sharing Agreements; Contracts
Local Government Agency	Law Enforcement Agencies	Yes	Health and Safety; Criminal Activity	Both PII & PHI	VHA Handbook 1605.1; Standing Letter Agreements
Research Entity	USC, UCLA Affiliates		Research activities for IRB and R&D Approved Protocols; Health & Safety	Both PII & PHI	VHA Handbook 1605.1 and 1907.1; Patient Authorization; Patient Care Referrals for Healthcare; Affiliate Agreement
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.

Access is authorized by Patient Consent and Authorization for Research Purposes; Business Associate Agreements; Contracts; Researchers; State Registries for Reporting Purposes with Standing Letter on File

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: The Vista database has specific fields that

How is data checked for completeness?

Answer: The data elements entered into the Vista

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

Answer: All entries must contain the date, time and

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

Answer: Health Information Professionals at the fa

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: SOR's are maintained 75 Years after the la

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

Answer: Title 44, Section 3301, of the United State

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

Answer: The RCS 10-1 contains retention and dispo

Where are these procedures documented?

Answer: www.1.va.gov/vhapublications/RCS10/rcs

How are data retention procedures enforced?

Answer: The Central Office Forms, Publications an

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:

All VHA employees are responsible for en

(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: Security monitoring, testing, and evaluations are required to be conducted on at least a quarterly basis to ensure that controls are in place and working properly.

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

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"/> Contingency Planning | <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: Collect minimum PII in all collection sources. Example: SSN Reduction Act

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 VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow NIST SP800-53 moderate impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of this facility' common security controls. These issues are identified and described in the system security plans for the individual information systems.

Please add additional controls: