

Welcome to the PIA for FY09!

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

e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies an individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirectly identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

(FY 09) PIA: System Identification

Program or System Name: REGION 1 > VHA > VISN 19 > Cheyenne VAMC > VistA - NT Cache

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

Description of System / Application / Program: Each Veterans Affairs (VA) medical center uses VistA Legacy (formerly DHCP, Decentralized Hospital C

Facility Name:

Title:	Name:	Phone:	Email:
Privacy Officer:	LaRoy Books	307.778.7550 x7	laroy.books@va.gov
Information Security Officer:	Jeff Ross	307.778.7343	jeff.ross@va.gov
Chief Information Officer:	Liz McCulloch	307.778.7568	liz.mcculloch@va.gov
Person Completing Document:			
Other Titles:			

Other Titles:

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY) 04/2008

Date Approval To Operate Expires: 04/2011

What specific legal authorities authorize this program or system: There is no SORN because the system is not a Privacy Act System of Records

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

20000

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.

N\A

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

Yes

If No, please explain:

Date of Report (MM/YYYY):

04/2009

If answers 'Yes' to one or more of the following, please check the appropriate box, continue to the next tab, and complete the remaining questions on this form. If none have been checked then skip to Signatures tab, obtain the appropriate signatures, and submit this document.

- Has a PIA NOT been completed within the last three years?
- 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?

(FY 09) 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: | Veterans Health Information System and Technology Architectu |
| 3. Location where the specific applicable System of Records Notice may be accessed (include the URL): | http://vaww.vhaco.va.gov/privacy/Update_SOR/SOR24VA19.pdf |

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 09) 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 messaged conveyed to them?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Verbal	The information is used in the routine course of business to provide medical care and reimbursement for insurance	Verbally
Family Relation (spouse, children, parents, grandparents, etc)	VA File Database	Their information remains confidential and contact purposes only	Verbally
Service Information	Paper	Used for eligibility for health care	Verbally
Medical Information	Electronic/File Transfer	The information is used to treat and care for the vetera	Automated
Criminal Record Information			
Guardian Information	Paper	This information is used in the notification process and as required for medical decisions.	Verbally
Education Information			
Benefit Information	Paper	This information is used for follow up care.	Automated
Other (Explain)	Paper	In addition insurance and employment information is available on the veteran for use in billing for care.	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?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	VA Files / Databases (Identify file)	Mandatory
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary
Service Information	Yes	Other (Explain)	Mandatory
Medical Information	Yes	Other Federal Agency (Identify)	Mandatory
Criminal Record Information			
Guardian Information	Yes	Other (Explain)	Voluntary
Education Information	No		
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory
Other (Explain)			
Other (Explain)	Yes	Veteran	Mandatory

Other (Explain)

How is a privacy notice provided?

Written

**Additional
Comments**

Military Records
DOD

Verbally by veterans
and outside sources
including VA
database

Other sources VA
State, federal,
multiple

It can come from all
sources

Insurance
Information
employment
information for use
in billing

(FY 09) 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	Veterans benefits Administration	Yes	Benefits	Both PII & PHI	Veterans rights
Other Veteran Organization	Veterans benefits Administration	Yes	Benefits	Both PII & PHI	Veterans rights
Other Federal Government Agency	Department of Defence	Yes	Medical Care	Both PII & PHI	Sharing agreement with DOD
State Government Agency	State health department	No	CDC	Both PII & PHI	State and federal laws
Local Government Agency					
Research Entity					
Other Project / System	State veterans homes	No	Health information	Both PII & PHI	State home program
Other Project / System					
Other Project / System					

(FY09) PIA: Access to Records

Does the system gather information from another system?
Please enter the name of the system:

No

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

(FY09) 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.

VA is authorized by VA 1605.1 handbook

Answer:

(FY 09) PIA: Program Level Questions

Does this PIA contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?	Yes
If Yes, Please Specify:	PII/PHI could cause harm to the VA if impr
Explain how collected data are limited to required elements:	
Answer:	limited to what is required
How is data checked for completeness?	
Answer:	Data is reviewed by staff and compared to
What steps or procedures are taken to ensure the data remains current and not out of date?	
Answer:	Clinical data is not removed. Administrati
How is new data verified for relevance, authenticity and accuracy?	
Answer:	New data is compared with printed form c
<i>Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)</i>	
Answer:	

(FY 09) PIA: Retention & Disposal

What is the data retention period?	
Answer:	Up to 75 years
Explain why the information is needed for the indicated retention period?	
Answer:	Federal Law mandates
What are the procedures for eliminating data at the end of the retention period?	
Answer:	Security level 6 shredding
Where are these procedures documented?	
Answer:	6500
How are data retention procedures enforced?	
Answer:	Records Management Responsibilities . The E

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 09) 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 09) 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:

This section applies to Regional Data Processing Center in Denver Colorado whe

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

Yes

If 'No' please describe why:

Answer:

This section applies to Regional Data Processing Center in Denver Colorado whe

Explain how the project meets IT security requirements and procedures required by federal law.

Answer:

This section applies to Regional Data Processing Center in Denver Colorado whe

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

- | | |
|---|--|
| <input type="checkbox"/> Air Conditioning Failure | <input type="checkbox"/> Hardware Failure |
| <input type="checkbox"/> Chemical/Biological Contamination | <input type="checkbox"/> Malicious Code |
| <input type="checkbox"/> Blackmail | <input 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"/> Data Integrity Loss | <input type="checkbox"/> Vandalism/Rioting |
| <input type="checkbox"/> Denial of Service Attacks | <input type="checkbox"/> Errors (Configuration and Data Entry) |
| <input type="checkbox"/> Earthquakes | <input type="checkbox"/> Burglary/Break In/Robbery |
| <input type="checkbox"/> Eavesdropping/Interception | <input type="checkbox"/> Identity Theft |
| <input type="checkbox"/> Fire (False Alarm, Major, and Minor) | <input type="checkbox"/> Fraud/Embezzlement |
| <input type="checkbox"/> Flooding/Water Damage | |

Answer: (Other Risks)

This section applies to Regional Data Processing Center in Denver Colorado where

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

- | | |
|--|--|
| <input type="checkbox"/> Risk Management | <input type="checkbox"/> Audit and Accountability |
| <input type="checkbox"/> Access Control | <input type="checkbox"/> Configuration Management |
| <input type="checkbox"/> Awareness and Training | <input type="checkbox"/> Identification and Authentication |
| <input type="checkbox"/> Contingency Planning | <input type="checkbox"/> Incident Response |
| <input type="checkbox"/> Physical and Environmental Protection | <input type="checkbox"/> Media Protection |
| <input type="checkbox"/> Personnel Security | |

Personnel Security

Certification and Accreditation Security Assessments

Answer: (Other Controls)

This section applies to Regional Data Processing Center in Denver Colorado where

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer:

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?
FALSE

Please add additional controls:

This section applies to Regional Data Processing Center in Denver Colorado whe

FY 09: 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 09) PIA: Final Signatures

Facility Name: 0

Title:	Name:	Phone:	Email:
Privacy Officer:	LaRoy Books	307.778.7550 x7012	laroy.books@va.gov
Digital Signature Block			
Information Security Officer:	Jeff Ross	307.778.7343	jeff.ross@va.gov
Digital Signature Block			
Chief Information Officer:	Liz McCulloch	307.778.7568	liz.mcculloch@va.gov
Digital Signature Block			
Person Completing Document:		0	0
Digital Signature Block			
System / Application / Program Manager:		0	0
Digital Signature Block			

Date of Report: 4/21/2009

OMB Unique Project Identifier 029-00-01-11-01-1180-00

Project Name

REGION 1 > VHA > VISN 19 >
Cheyenne VAMC > VistA - NT Cache