

### **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://vawww.privacy.va.gov/Privacy\\_Impact\\_Assessments.asp](http://vawww.privacy.va.gov/Privacy_Impact_Assessments.asp)

### **Roles and Responsibilities:**

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the Privacy Impact Assessment Handbook 6202.2 referenced in the procedure section of this document.

- a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Handbook 6202.2.
- b. Records Officer is responsible for supplying records retention and deletion schedules.
- c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Handbook 6202.2 and to immediately report all anomalies to the Privacy Service and appropriate management chain.
- d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.
- e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and

systems, coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues, and reviewing and approving the PIA before submission to the Privacy Service.

**Definition of PII (Personally Identifiable Information)**

Information in identifiable form that is collected and stored in the system that either directly identifies 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: PROGRAM OFFICE>VHA>VISN 00>HINES CMOP>VISTA DR

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

Exhibit 300 - 029-00-01-11-01-1180-00

The National CMOP VISTA system receives batch transmissions of prescription data from the VA Medical Facilities VISTA systems daily utilizing TCP/IP interface through the Frame Relay T1 line via MailMan. The batch transmissions are then downloaded from the National CMOP VISTA to the Centralized Database Server via flat file transfer. The Centralized Database Server then downloads the batch files to each CMOP Prescription Processing System via flat file. The Hines VISTA DR system is used as a backup to the Tucson VISTA system for contingency purposes.

Description of System / Application / Program:

---

Facility Name: Consolidated Mail  
Outpatient Pharmacy

Title:	Name:	Phone:	Email:
Privacy Officer:	LaRue Roberts	361-356-1269	<a href="mailto:larue.morian2@va.gov">larue.morian2@va.gov</a>
Information Security Officer:	Yancy McPherson	843-745-8648	<a href="mailto:Yancy.McPherson@va.gov">Yancy.McPherson@va.gov</a>
Chief Information Officer:	Phil Burkhalter	520-209-3118	<a href="mailto:Phil.Burkhalter@va.gov">Phil.Burkhalter@va.gov</a>
Person Completing Document:	LaRue Roberts	361-356-1269	LaRue.Morian2@va.gov
Other Titles:	Jennifer Tidrick	615-225-4594	<a href="mailto:Jennifer.Tidrick@va.gov">Jennifer.Tidrick@va.gov</a>

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:

Title 38, United States Code, Section 7301 (a)

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

500,000 patients over a 45 day period then the data is then purged daily as the prescription is filled and the filling data is transferred back to the medical centers.

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.

14 years

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): 05/2009

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?

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):
2. Name of the System of Records:
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)?

---

Does the System of Records Notice require modification or updating?

---

Is PII collected by paper methods?

Is PII collected by verbal methods?

Is PII collected by automated methods?

Is a Privacy notice provided?

Proximity and Timing: Is the privacy notice provided at the time of data collection?

Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

---

---

Yes

---

79VA19  
VistA-VA

[http://vaww.vhaco.va.gov/privacy/Update\\_SOR/ListVHASORS](http://vaww.vhaco.va.gov/privacy/Update_SOR/ListVHASORS)

---

Yes

---

No

---

***(Please Select Yes/No)***

No

No

Yes

Yes

Yes

Yes

Yes

---

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 message conveyed to them?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	VA File Database	Information required to process and fill prescriptions	Verbally
Family Relation (spouse, children, parents, grandparents, etc)			
Service Information			
Medical Information	VA File Database	Information required to process and fill prescriptions	Verbally
Criminal Record Information			
Guardian Information			
Education Information			
Benefit Information			
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?

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)

No

Service Information

No

Medical Information

Yes

VA Files / Databases (Identify file)

Mandatory

Criminal Record Information

No

Guardian Information

No

Education Information

No

Benefit Information

No

Other (Explain)

Other (Explain)

Other (Explain)

---

---

**How is a privacy  
notice provided?**

---

Verbally

---

---

---

Verbally

---

---

---

---

---

---

---

**Additional  
Comments**

---

Data purged daily  
after prescription is  
filled and fill data  
transferred back to  
medical center.



Data purged daily  
after prescription is  
filled and fill data  
transferred back to  
medical center.



(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					
Other Veteran Organization					
Other Federal Government Agency					
State Government Agency					
Local Government Agency					
Research Entity					
Other Project / System					
Other Project / System					
Other Project / System					

(FY09) PIA: Access to Records

Does the system gather information from another system? Yes

Please enter the name of the system: VA Medical Facilities VISTA systems

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

(FY09) PIA: Secondary Use

Will PII data be included with any secondary use request?

No

- Drug/Alcohol Counseling
- Mental Health
- HIV
- Research
- Sickle Cell
- Other (Please Explain)

if yes, please check all that apply:

Describe process for authorizing access to this data.

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?

No

If Yes, Please Specify:

---

Explain how collected data are limited to required elements:

Answer: The CMOP software limits the data elements to those that are needed to fill the prescription. Only those data elements are transmitted to the CMOP. If a problem is encountered with the data elements the data will not transmit to the CMOP. The medical center will receive an error message. The CMOP Production server will only accept specific data elements required to process the prescription. CMOP users do not have the ability to modify any of the data elements received from the Medical Center.

---

How is data checked for completeness?

Answer: The CMOP Transmission Acknowledgment message is created by the host CMOP software when the data transmissions are received data is validated, and loaded into safe storage in the CMOP database by the CMOP VistA software. Initially the message is delivered to the remote medical center to the PSXMAIL key holders to indicate that the CMOP has successfully received the data transmitted. The message is also delivered to the medical center CMOP server software and is used to file the date and time the data was received at the CMOP in the transmission entry in the CMOP TRANSMISSION file (#550.2). Receipt of both the Transmission Confirmation and the Transmission Acknowledgment messages for a single transmission confirm that the data transmitted and downloaded to the CMOP facility successfully. The medical center CMOP software will screen prescriptions suspended for transmissions for all of the appropriate data elements. If any are missing the prescription will not be transmitted. Once the data is received by CMOP it is automatically handed to the Prescription Processing System. If any data elements are missing or incorrect, the prescription will be automatically suspended and will not process. Suspended prescriptions are reviewed and cancelled back to the medical center daily.

---

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

Answer: Transmissions are automatically queued daily at the Medical Center. The CMOP (Batch Number) from (Site) Received message is created when data is downloaded successfully into the CMOP database files at the host facility. This message informs the CMOP personnel that a transmission has arrived and is ready to transfer to the automated vendor system. All batch numbers are a unique identifier. The CMOP software will alert staff when data is not current. The CMOP Acknowledgement not Received message is sent when a Transmission Acknowledgement message has not been received for a previous transmission after 24 hours. The CMOP software checks each transmission entry in the CMOP TRANSMISSION file (#550.2) 24 hours after the data is transmitted to ensure that the data was received at the CMOP host facility. If an acknowledgement date/time has not been filed for the transmission, this message reminds the key holders that the Transmission Acknowledgement message has not yet been received. CMOP and VA Medical Center staff review the transmission logs daily to ensure that we have current prescription data to process.

---

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

Answer: The CMOP Error Encountered message is created when medical center CMOP transmission data has been handed to MailMan for delivery to the CMOP host facility. This message is a direct result of the CMOP software screening prescriptions suspended for CMOP during data transmission. If a problem is detected with a prescription selected for transmission, the prescription is not transmitted to the CMOP, but is noted in this message to the user to provide information to correct the problem. If the data is corrected as noted in this message, the prescription will be included in the next transmission. If the data problem is not corrected, the prescription will continue to be listed in this message each time a transmission is initiated. If the data is not corrected the prescription will never be transmitted. The CMOP Error Encountered message may be sent in varying formats depending on the data problems to be reported.

---

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

Answer:

---

## (FY 09) 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: Pharmaceutical care

---

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

Answer: Comply with VA regulations that address sanitization and disposal of VA data.

---

Where are these procedures documented?

Answer: VA Directive and Handbook 6500. NIST guidance.

---

How are data retention procedures enforced?

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

---

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:

---

---

---

---

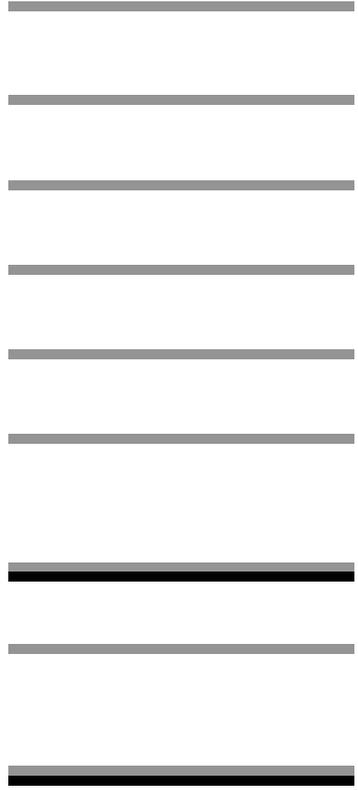
---

\_\_\_\_\_

\_\_\_\_\_

**\_\_\_\_\_**

\_\_\_\_\_



## (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:

---

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: This system works in conjunction with strong authentication measures to ensure and authenticate the identification of VA network users. System interconnection agreement (SIA)s are a system level measure to ensure that all interconnected systems meet minimum VA access policies for interconnected systems from within and outside the VA wide area network (WAN) boundaries. Moreover, the VA employs a comprehensive incidence response unit to respond to unwanted incursions and institutes enterprise level ant-virus system to protect mission critical applications on the desktop. Finally, the VA security program is an iterative program with repeatable processes that, in an ongoing basis, will mitigate vulnerabilities, minimize security exposures and maintain security and operating risk at acceptable levels. NIST 800-53 security controls are in place and tested every three years or as needed.

---

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 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) |

- Denial of Service Attacks
- Earthquakes
- Eavesdropping/Interception
- Fire (False Alarm, Major, and Minor)
- Flooding/Water Damage
- Errors (Configuration and Data Entry)
- Burglary/Break In/Robbery
- Identity Theft
- Fraud/Embezzlement

Answer: (Other Risks)

---

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

- Risk Management
- Access Control
- Awareness and Training
- Contingency Planning
- Physical and Environmental Protection
- Personnel Security
- Certification and Accreditation Security Assessments
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Media Protection

Answer: (Other Controls)

---

## PIA: PIA Assessment

---

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

Answer: None

---

**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 09) PIA: Final Signatures

Facility Name: Consolidated Mail Outpatient Pharmacy

Title:	Name:	Phone:
Privacy Officer:	LaRue Roberts	361-356-1269
Digital Signature Block		
Information Security Officer:	Yancy McPherson	843-745-8648
Digital Signature Block		
Chief Information Officer:	Phil Burkhalter	520-209-3118
Digital Signature Block		
Person Completing Document:	LaRue Roberts	361-356-1269
Digital Signature Block		
System / Application / Program Manager:	Jennifer Tidrick	615-225-4594
Digital Signature Block		

Date of Report: 5/1/2009

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

Project Name PROGRAM OFFICE>VHA>VISN 00>HINES CMOP>VISTA DR

Email:

larue.morian2@va.gov

Yancy.McPherson@va.gov

Phil.Burkhalter@va.gov

Larue.Morian2@va.gov

Jennifer.Tidrick@va.gov

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.

---



























