

## **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.

Information Security Officer (ISO) is responsible for assessing the risks, control and protecting 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 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, indirect 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: Lab Replacement Project

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

029-00-01-11-01-1222-00

The purpose of this project is to replace the legacy laboratory information management system (LIMS) with a Commercial Off-The-Shelf (COTS) LIMS. The selected COTS product, Cerner Millennium PathNet that resides at the Regional Data Processing Center, will allow the VA to meet future requirements of Electronic Medical Record, HealthVet and interoperability between DoD and PHS as per public law 107-287. The VHA Laboratory Service is a critical part of offering high quality clinical care to veterans. Almost 80% of clinical decisions are based on the patient's laboratory test results which have increased an average of 5% annually and approximately 30% since 2001. The selected COTS replacement exceeds the functional requirements of the VA Laboratory community, supports the reengineered business processes, requires no software code modifications to the COTS LIMS and will move laboratory information from locally maintained records to "patient focused" (portability of information to another facility). The project supports the VA strategic goal of providing high-quality, reliable, accessible, timely, and efficie

Description of System / Application / Program:

---

Facility Name:

Title:	Name:	Phone:	Email:
Privacy Officer:			
Information Security Officer:			
Chief Information Officer:			
Person Completing Document:	Bonnie Brown	662.843.5105	<a href="mailto:bonnie.brown3@va.gov">bonnie.brown3@va.gov</a>
Program Manager:	Cheryl Latham	518.499.0263	<a href="mailto:cheryl.latham@va.gov">cheryl.latham@va.gov</a>
VHA HDI Security Security Engineer:	Scott Rogers	404.828.5212	<a href="mailto:scott.rogers@va.gov">scott.rogers@va.gov</a>
Other Titles:			
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	08/2008		
Date Approval To Operate Expires:			

---

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: 1,000,000 - 9,999,999

Identify what stage the System / Application / Program is at: Development/Acquisition

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. 04/2010

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): 12/2008

**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):

24VA19

2. Name of the System of Records:

Patient Medical Records-VA

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

<http://vaww.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?

No

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

No

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

No

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?

---

## (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?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Electronic/File Transfer	Electronic/File transfer refers to messaging between applications to exchange information. Veteran/primary subjects are not part of this process and as such, receive no notification of information transfers between applications.		
Family Relation (spouse, children, parents, grandparents, etc)	Electronic/File Transfer	Electronic/File transfer refers to messaging between applications to exchange information. Veteran/primary subjects are not part of this process and as such, receive no notification of information transfers between applications.		
Service Information	Electronic/File Transfer	Electronic/File transfer refers to messaging between applications to exchange information. Veteran/primary subjects are not part of this process and as such, receive no notification of information transfers between applications.		
Medical Information	Electronic/File Transfer	Electronic/File transfer refers to messaging between applications to exchange information. Veteran/primary subjects are not part of this process and as such, receive no notification of information transfers between applications.		
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?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	Cerner Millennium PathNet will receive data from the laboratory automated instruments through electronic interface and from VistA Legacy using HL7. (1) VistA File #2 Patient: Ensure laboratory tests are performed and verified results are reported on the right patient record. (2) VistA File #200 New Person: Ensure proper documentation of authorized personnel are correctly identified and recorded on the patient's record when performing the associated work effort. Includes laboratory staff, ordering providers, and persons responsible for performing specimen collection and point of care testing. (3) MPI Veteran/Client File #985: Ensure proper updates to a patient's identity traits are stored on the correct patient record. Specific fields can be found at <a href="http://vista.med.va.gov/mpi/primary_view_ID_traits.asp">http://vista.med.va.gov/mpi/primary_view_ID_traits.asp</a>
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Medical Information	Yes	Other (Explain)	Mandatory	results from analyzers and manual tests

Criminal Record Information No

Guardian Information No

Education Information No

Benefit Information No

Other (Explain)

Other (Explain)

Other (Explain)

## (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					
Private Reference Lab	Quest Diagnostics Reference Lab	Yes	Lab orders may be transmitted to and results transmitted from Quest if the facility uses a reference lab.	Both PII & PHI	national contract and MOU put in place for the entire VHA
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 VistA, MPI
Does the system gather information from an individual?	No
If information is gathered from an individual, is the information provided:	<input type="checkbox"/> Through a Written Request <input type="checkbox"/> Submitted in Person <input type="checkbox"/> 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:

Cerner Millennium PathNet is defined by specific files, tables and fields that store data used or produced by the laboratory information system. The system architecture and database environment rules are incorporated in Cerner Millennium PathNet.

---

Answer:

How is data checked for completeness?

Answer:

Cerner Millennium PathNet contains specific field definitions and algorithms that check for completeness of data. Cerner Millennium PathNet supports the entry of numeric, calculation, alpha, date, free text, text, and interpretation result types. Numeric result formats are mapped according to medical device or methodology specifications. Alpha result options for a procedure can be limited to a subset of alpha responses. Calculations are automatically performed when all the component tests are resulted. Interpretations can be system-generated to produce the textual and/or alpha results triggered by the results of the component tests. Both calculations and interpretations can be performed through the use of a result entry function; calculations can also be performed through the use of a medical device interface. The database standards are incorporated in the Cerner Millennium PathNet and are repudiated using Health Level 7 (HL7) messaging standards.

---

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

Answer:

Cerner Millennium PathNet is integrated with VistA applications that ensure complete and accurate availability of data and will store data that is date and time stamped. VistA will transmit to Cerner Millennium PathNet provider, admission, discharge, transfer and registration updates. Laboratory information system is designed to meet Privacy Act, HIPAA legislation and NIST standards as well as project specific architecture and database standards.

---

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

Answer:

Cerner's auditing solution was designed in response to HIPAA privacy and security provisions, among other considerations, allowing the audit of user actions as patient-identifiable information is accessed. This information includes data identifying the user, the patient, the context of the access, and the actions performed to the patient data, including actions that create, verify, modify, complete, amend\error correct, and print patient information. The system validates results and alerts users when results exceed reference ranges, critical limits, review limits, linear limits and delta check parameters.

---

*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:

Clinical information is retained in accordance with VA Records Control Schedule 10-1.

---

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

Answer:

Demographic Information is updated as applications for care are submitted and retained in accordance with VA Records Control Schedule 10-1. Retention period for the PH is 75 years.

---

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

Answer:

Electronic Final Version of Patient Medical Record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records Control Schedule 10-1, Item XUII, 2.b

---

Where are these procedures documented?

Answer:

VA Handbook 6300; Record Control Schedule 10-1

---

How are data retention procedures enforced?

Answer:

VA Records Control Schedule 10-1, Records Management Responsibilities

---

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

The Health Information Resources Service (HIRS) is responsible for developing policies and procedures for effective and evident records management throughout VHA. In addition, HIRS acts as the liaison between VHA and National Archives and Records Administration (NARA) on issues pertaining to records management practices and procedures. Field records officers are responsible for records management activities at their facilities. Program officials are responsible for creating, maintaining, protecting, and disposing of records in their program area in accordance with NARA regulations and VA policy. All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures.

---

*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: Account access is reviewed monthly. Security evaluation is an on-going process

---

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)

---

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)

---

## 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?

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: 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.

---

System of Records:

Is PII collected by paper methods?

If VistA is down but the Cerner system is up, orders may be written on paper and manually entered into Cerner.

Is a Privacy notice provided?

Proximity and Timing:

The VA consent form (VA Form 1010EZ) is signed by the patient upon request for care. The text on the consent form includes notice of Privacy Act Information. Patients are provided VA Notice of Privacy Practices at that time and not for each lab test ordered.

# (FY 09) PIA: Final Signatures

Facility Name:

0

Title:	Name:	Phone:	Email:
Privacy Officer:		0	0

Information Security Officer:

Don Bulluss

802-280-6665

don.bulluss@va.gov



Chief Information Officer:

0

0

0

Person Completing Document:

Bonnie Brown

662.843.5105

bonnie.brown3@va.gov

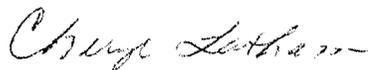


System / Application / Program Manager:

Cheryl Latham

518.499.0263

cheryl.latham@va.gov



Date of Report:

12/2008

OMB Unique Project Identifier

029-00-01-11-01-1222-00

Project Name

Lab Replacement Project