

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/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 reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or

(FY 2010) PIA: System Identification

Program or System Name: Laboratory System Reengineering Project

OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-01-11-01-1222-00

Description of System / Application / Program: 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 is Cerner Millennium PathNet, which will be hosted at the Kansas City Cerner facility. The LIMS will bring VA Labs in compliance with Joint Commission and regulatory guidelines; enhance Laboratory business processes; meet emerging technology needs (e.g. Molecular Diagnostics, Synoptic Reporting); provide flexible and timely response to change (clinical, business, regulatory); improve Data Sharing and Interoperability with DoD, Public Health Labs and reference labs; increase levels of standardization across Pathology & Laboratory Medicine Service; and support the distributed Remote Data Processing Center model. The VHA Laboratory Service is a critical part of offering high quality clinical care to veterans. Benefits to the veteran include increased access and exchange of lab data by providing an industry-leading, standardized LIMS that supports improved clinical diagnostic services, faster processing and reporting of lab tests and correction of identified patient safety deficiencies. The Service relies heavily on information technology to support all phases of lab activities, from specimen collection to dissemination of results. The selected LIMS, with hundreds of existing implementations, exceeds the functional requirements of the VA Laboratory community, supports reengineered business processes, requires no software modifications to the COTS LIMS and will move laboratory information from “facility focused” (records maintained locally) to “patient focused” (portability of information to another facility). The project supports the VA strategic goal of providing high-quality, reliable, accessible, timely, and efficient health care that maximizes the health and functional status of veterans.

Facility Name:

Title:	Name:	Phone:	E-mail
Privacy Officer:	Dennis Stewart	202.461.7456	dennis.stewart2@va.gov
Information Security Officer:	Don Bulluss	802.280.6665	don.bulluss@va.gov
System Owner:	Lorraine Landfried	202.245.4020	lorraine.landfried@va.gov
Person Completing Document:	Bonnie Brown	662.545.4974	bonnie.brown3@va.gov
Senior Program Manager	Cheryl Latham	518.499.0263	cheryl.latham@va.gov

VHA HDI Security Security Engineer:	Scott Rogers	404.828.5212	scott.rogers@va.gov
Deputy Director Certification Office	Dirk Barrineau	304.262.7654	dirk.barrineau@va.gov
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	05/2009		
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: 01/2011

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):

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 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): | 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://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?

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 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)	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.	Automated	Automated
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.	Automated	Automated
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.	Automated	Automated
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.	Automated	Automated

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 http://vista.med.va.gov/mpi/primary_view_ID

Family Relation (spouse,
children, parents,
grandparents, 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 http://vista.med.va.gov/mpi/primary_view_ID

Service Information

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 http://vista.med.va.gov/mpi/primary_view_ID results from analyzers and manual tests

	Yes	VA Files / Databases (Identify file)	Mandatory
Medical Information	Yes	Other (Explain)	Mandatory
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	VHA	Yes	patient electronic Laboratory data to VAMCs caring for patient	Both PII & PHI	BAA with Cerner
Other Veteran Organization		No			
Other Federal Government Agency	DoD	No	exchange electronic laboratory test data	Both PII & PHI	Cerner is a Business Associate of VHA and has signed a legally binding and HIPAA compliant Business Associate Agreement
State Government Agency		No			
Local Government Agency		No			
Research Entity		No			
Private Reference Lab	Quest Diagnostics and LabCorp reference labs	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 are in place for the entire VHA
Other Project / System	LabCorp	Yes	Lab orders may be transmitted to and results transmitted from Data Corp if the facility uses a reference lab.	Both PII & PHI	MOU in place with Huntington VAMc (alpha site)
Other Project / System	Cerner remote hosting facility in Kansas City	Yes	lab orders and results are stored and transmitted to VistA	Both PII & PHI	VA contract in place

(FY 2010) PIA: Access to Records

Does the system gather information from another system? Yes

Please enter the name of the system: VA VistA, MPI
Cerner Remote Hosting facility

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 via Request
 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

if yes, please check all that apply:
 Drug/Alcohol Counseling Mental Health HIV
 Research Sickle Cell Other (Please Explain)

Describe process for authorizing access to this data.

Answer:

(FY 2010) PIA: Program Level Questions

Does this PIA 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 interfaced 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 2010) 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 XVII, 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)

Yes

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

Answer:

(COPPA)

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

No

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

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.
no change

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.

FALSE

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.

FALSE

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.

FALSE

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.

FALSE

Please add additional controls:

(FY 2010) PIA: VISTA Minor Applications

Explain what minor application that are associated with your installation? *(Check all that apply)*

ACCOUNTS RECEIVABLE	DRUG ACCOUNTABILITY	INCOMPLETE RECORDS TRACKING	ONCOLOGY	SCHEDULING
ADP PLANNING (PLANMAN)	DSS EXTRACTS	INPATIENT MEDICATIONS	ORDER ENTRY/RESULTS REPORTING	SECURITY SUITE UTILITY PACK
ADVERSE REACTION TRACKING	EDUCATION TRACKING	INTAKE/OUTPUT	OUTPATIENT PHARMACY	SHIFT CHANGE HANDOFF TOOL
ASISTS	EEO COMPLAINT TRACKING	INTEGRATED BILLING	PAID	SOCIAL WORK
AUTHORIZATION/SUBSCRIPTION	ELECTRONIC SIGNATURE	INTEGRATED PATIENT FUNDS	PATCH MODULE	SPINAL CORD DYSFUNCTION
AUTO REPLENISHMENT/WARD STOCK	ENGINEERING	INTERIM MANAGEMENT SUPPORT	PATIENT DATA EXCHANGE	SURGERY
AUTOMATED INFO COLLECTION SYS	ENROLLMENT APPLICATION SYSTEM	KERNEL	PATIENT FEEDBACK	SURVEY GENERATOR
AUTOMATED LAB INSTRUMENTS	EQUIPMENT/TURN-IN REQUEST	KIDS	PATIENT REPRESENTATIVE	TEXT INTEGRATION UTILITIES
AUTOMATED MED INFO EXCHANGE	EVENT CAPTURE	LAB SERVICE	PCE PATIENT CARE ENCOUNTER	TOOLKIT
BAR CODE MED ADMIN	EVENT DRIVEN REPORTING	LETTERMAN	PCE PATIENT/IHS SUBSET	UNWINDER
BED CONTROL	EXTENSIBLE EDITOR	LEXICON UTILITY	PHARMACY BENEFITS MANAGEMENT	UTILIZATION MANAGEMENT ROLLUP
BENEFICIARY TRAVEL	EXTERNAL PEER REVIEW	LIBRARY	PHARMACY DATA MANAGEMENT	UTILIZATION REVIEW
CAPACITY MANAGEMENT - RUM	FEE BASIS	LIST MANAGER	PHARMACY NATIONAL DATABASE	VA CERTIFIED COMPONENTS - DSSI
CAPACITY MANAGEMENT TOOLS	FUNCTIONAL INDEPENDENCE	MAILMAN	PHARMACY PRESCRIPTION PRACTICE	VA FILEMAN
CARE MANAGEMENT	GEN. MED. REC. - GENERATOR	MASTER PATIENT INDEX VISTA	POLICE & SECURITY	VBECs

	CLINICAL CASE REGISTRIES		GEN. MED. REC. - I/O		MCCR NATIONAL DATABASE		PROBLEM LIST		VDEF
	CLINICAL INFO RESOURCE NETWORK		GEN. MED. REC. - VITALS		MEDICINE		PROGRESS NOTES		VENDOR - DOCUMENT STORAGE SYS
	CLINICAL MONITORING SYSTEM		GENERIC CODE SHEET		MENTAL HEALTH		PROSTHETICS		VHS&RA ADP TRACKING SYSTEM
	CLINICAL PROCEDURES		GRECC		MICOM		QUALITY ASSURANCE INTEGRATION		VISIT TRACKING
	CLINICAL REMINDERS		HEALTH DATA & INFORMATICS		MINIMAL PATIENT DATASET		QUALITY IMPROVEMENT CHECKLIST		VISTALINK
	CMOP		HEALTH LEVEL SEVEN		MYHEALTHEVET		QUASAR		VISTALINK SECURITY
	CONSULT/REQUEST TRACKING		HEALTH SUMMARY		Missing Patient Reg (Original) A4EL		RADIOLOGY/NUCLEAR MEDICINE		VISUAL IMPAIRMENT SERVICE TEAM ANRV
	CONTROLLED SUBSTANCES		HINQ		NATIONAL DRUG FILE		RECORD TRACKING		VOLUNTARY TIMEKEEPING
	CPT/HCPCS CODES		HOSPITAL BASED HOME CARE		NATIONAL LABORATORY TEST		REGISTRATION		VOLUNTARY TIMEKEEPING NATIONAL
	CREDENTIALS TRACKING		ICR - IMMUNOLOGY CASE REGISTRY		NDBI		RELEASE OF INFORMATION - DSSI		WOMEN'S HEALTH
	DENTAL		IFCAP		NETWORK HEALTH EXCHANGE		REMOTE ORDER/ENTRY SYSTEM		Care Tracker
	DIETETICS		IMAGING		NOIS		RPC BROKER		
	DISCHARGE SUMMARY		INCIDENT REPORTING		NURSING SERVICE		RUN TIME LIBRARY		
	DRG GROUPER		INCOME VERIFICATION MATCH		OCCURRENCE SCREEN		SAGG		

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name	Description	Comments
LEDI	Laboratory Electronic Data Interchange	

Minor app #1

yes Is PII collected by this minor application?

no Does this minor application store PII?

If yes, where?

Who has access to this d this is a tool for LSRP to

Name	Description	Comments

Minor app #2

yes Is PII collected by this min or application?

no Does this minor application store PII?

yes If yes, where?

no Who has access to this d

Name	Description	Comments

Minor app #3

yes Is PII collected by this min or application?

no Does this minor application store PII?

yes If yes, where?

no Who has access to this d

(FY 2010) PIA: Minor Applications

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

Minor app #1	Name		Description		Comments
		yes no	Is PII collected by this min or application?		
		yes no	Does this minor application store PII?		
			If yes, where?		
		Who has access to this data?			
Minor app #2	Name		Description		Comments
		yes no	Is PII collected by this min or application?		
		yes no	Does this minor application store PII?		
			If yes, where?		
		Who has access to this data?			
Minor app #3	Name		Description		Comments
		yes no	Is PII collected by this min or application?		
		yes no	Does this minor application store PII?		
			If yes, where?		
		Who has access to this data?			

(FY 2010) PIA: Additional Comments

Add any additional comments on this tab for any question in the form you want to comment on.

Please indicate the question you are responding to and then add your comments.

System of Records:

Is PII collected by paper methods?

If Vista is down and Cerner is up, orders may be written on paper and then manually entered into Cerner.

Is Privacy notice provided?

Proximity and Timing:

The VA consent form VA Form 1010EZ is signed by the patient upon request for care.

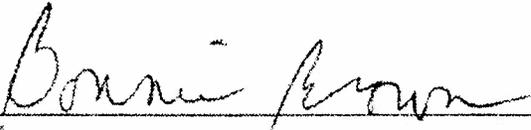
The text on the consent form includes notice of Privacy Act information.

Patients are provided a copy of VA Notice of Privacy Practices at that time and not for each test ordered.

(FY 2010) PIA: Final Signatures

Facility Name:

0

Title:	Name:	E-mail
Privacy Officer:	Dennis Stewart 202.461.7456	dennis.stewart2@va.gov
Digital Signature Block		
Information Security Officer:	Don Bulluss 802.280.6665	don.bulluss@va.gov
Digital Signature Block		
System Owner:	Lorraine Landfried 202.245.4020	lorraine.landfried@va.gov
		
Person Completing Document:	Bonnie Brown 662.545.4974	bonnie.brown3@va.gov
		
System / Application / Program Manager:	Cheryl Latham 518.499.0263	cheryl.latham@va.gov
		

Date of Report:

8/13/2010

OMB Unique Project Identifier

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

Project Name

Laboratory System Reengineering
Project