

## **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](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 combined, indirect identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

### **Macros Must Be Enabled on This Form**

To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

## (FY 2010) PIA: System Identification

**Program or System Name:** Region 4>VHA>VISN 04>Wilkes-barre HCS>LAN  
**OMB Unique System / Application / Program Identifier (AKA: UPID #):** 029-00-02-00-01-1120-00-404-143  
**Description of System / Application / Program:** The VA Medical Center Wilkes-Barre VAMCWB uses the Local Area Network (LAN) as a General Support System, supporting mission-critical and other systems necessary to conduct day-to-day operations within the Veterans Health Administration. Applications and devices within the LAN support numerous areas, including medical imaging, supply management, decision support, education and research. The Wilkes-barre VAMC's primary LAN infrastructure is composed of Wired and Wireless Cisco networks, medical and non-medical computing servers, PC workstations, thin clients, mobile computing devices and a centralized storage area network (SAN) with backup capabilities. Combined these systems are referred to as the Wilkes-Barre Local Area Network.

**Facility Name:** VA Medical Center, Wilkes-Barre, PA

<b>Title:</b>	<b>Name:</b>	<b>Phone:</b>	<b>Email:</b>
Privacy Officer:	Sharon Czuk	570-821-3521x4	<a href="mailto:sharon.czuk2@va.gov">sharon.czuk2@va.gov</a>
Information Security Officer:	Edward Wademan	570-821-3521x7	<a href="mailto:edward.wademan@va.gov">edward.wademan@va.gov</a>
Chief Information Officer:	David Longmore	570-821-7286	<a href="mailto:david.longmore@va.gov">david.longmore@va.gov</a>
Person Completing Document:	Edward Wademan	570-821-3521x7	<a href="mailto:edward.wademan@va.gov">edward.wademan@va.gov</a>
Other Titles:			

Other Titles:

Other Titles:

Date of Last PIA Approved by VACO Privacy

Services: (MM/YYYY) 08/2009

Date Approval To Operate Expires: 08/2011

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:

The VA Medical Center Wilkes-Barre (VAMCWB) LAN provides access and authentication to allow a user to interface with VAMCWB VistA system resources. VAMCWB VistA stores the personal information of more than 200,000 individuals. It also supports the business functions and provides network storage for over 1400 employees working at VAMCWB.

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.

Fully operational for approximately 20 + years.

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

Yes

If No, please explain:

Has a PIA been completed within the last three years?

Yes

Date of Report (MM/YYYY):

12/2009

**Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.**

- Have any changes been made to the system since the last PIA?
- Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- Does this system/application/program collect, store or disseminate PII/PHI data?
- Does this system/application/program collect, store or disseminate the SSN?

**If there is no Personally Identifiable Information on your system , please skip to TAB 12. ( See Comment for Definition of PII)**

## (FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?

Yes

if the answer above is no, please skip to row 16.

For each applicable System(s) of Records, list:

- |   |   |
|---|---|
| 1. All System of Record Identifier(s) (number):   | 79VA19/24VA19   |
| 2. Name of the System of Records:   | VistA-VA<br><a href="http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm">http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm</a> |
| 3. Location where the specific applicable System of Records Notice may be accessed (include the URL): | <a href="http://vaww.vhaco.va.gov/privacy/Update_SOR/SOR24VA19.pdf">http://vaww.vhaco.va.gov/privacy/Update_SOR/SOR24VA19.pdf</a>   |

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?

Yes

Does the System of Records Notice require modification or updating?

No

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

Is PII collected by paper methods?

Yes

Is PII collected by verbal methods?

Yes

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

Yes

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

Yes

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

Yes

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

Yes

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

Yes

## (FY 2010) PIA: Notice

Please fill in each column for the data types selected.

<b>Data Type</b>	<b>Collection Method</b>	<b>What will the subjects be told about the information collection?</b>	<b>How is this message conveyed to them?</b>	<b>How is a privacy notice provided?</b>
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Verbal	Administrative data is frequently de-identified and aggregated by business units and Quality Assurance to ensure that appropriate medical care is being provided to patients. This information is used by the business office to ensure that billing is accurate and to contact patients about appointments and scheduled admissions. Clinical data is used to track provider and facility compliance with national, regional and local performance measures. In addition, a complete copy of the medical database is maintained to ensure continuity of operations in the event that the primary Hospital Information System is unavailable for processing. Research data is made available to authorize researchers through our corporate data warehouse. In addition, data extracted from the data warehouse by researchers is stored on our Storage Area Network (SAN) and research servers for analysis.	Verbally	Written
Family Relation (spouse, children, parents, grandparents, etc)	Verbal	Dependent information such as Next of Kin or dependent children may be used to notify the family in the event of an adverse event, patient death, or need to secure a consent for a medical procedure or discharge planning.	Verbally	Written

Service Information	Electronic/File Transfer	Military Service Information (Branch of service, discharge date, discharge type, service connection rating, medical conditions related to military service, etc). This information is collected to assess eligibility for VA healthcare benefits and type of healthcare needed.	Verbally	Written
Medical Information	Electronic/File Transfer	Clinical data is used to track provider and facility compliance with national, regional and local performance measures. In addition, a complete copy of the medical database is maintained to ensure continuity of operations in the event that the primary Hospital Information System is unavailable for processing.	Verbally	Written
Criminal Record Information	Electronic/File Transfer	Criminal record information used by the VA Police to ensure provider and patient safety in the facility.	Verbally	Written
Guardian Information	Paper	This information is used in the notification process and as required for medical decisions.	Verbally	Written
Education Information	Paper	This information may also be used by the research programs to determine if there is a correlation between level of patient education and effectiveness of treatment. The resulting improvement in medical care is a key component of the VA mission.	Verbally	Written
Benefit Information	VA File Database	Benefits	Verbally	Written
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	No	Veteran	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	No	Veteran		
Service Information	No	Veteran	Mandatory	
Medical Information	No	VA Files / Databases (Identify file)		
Criminal Record Information	No	Other Federal Agency (Identify)		
Guardian Information	No	Other (Explain)		
Education Information	No	Veteran		
Benefit Information	No	VA Files / Databases (Identify file)		
Other (Explain)				The Department of Veterans Affairs Security Management and Reporting Tools (SMART) includes all I.T. Windows servers (including the file servers) as part of the LAN system. In addition to PKI and RMS, one of the VA's approved methods for the transfer of sensitive data is through the use of a Windows file share.
Other (Explain)				
Other (Explain)				

(FY 2010) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VBA/VA/Veterans Centers	Yes	Clinical and Administrative data for the purpose of ensuring benefits are received	Both PII & PHI	VHA Handbook 1605.1
Other Veteran Organization	BVA	No			
Other Federal Government Agency	Dod/CDC/SSA	No	Have DUAs in place for more than 3 years through the FHIE/BHIE Program	Both PII & PHI	DUA and VHA Handbook 1605.1
State Government Agency	State Veterans Home	No	Clinical data about patients that are common to both systems to provide effective, quality care across the continuum of treatment	Both PII & PHI	Contract
Local Government Agency		No			
Research Entity	HERL	No	Research	Both PII & PHI	VA Consent Form/HIPAA Authorization
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2010) PIA: Access to Records

Does the system gather information from another system? Yes

Please enter the name of the system: VistA/CPRS or PVTS

Per responses in Tab 4, does the system gather information from an individual? Yes

If information is gathered from an individual, is the information provided:

- Through a Written Request
- Submitted in Person
- Online via Electronic Form

Is there a contingency plan in place to process information when the system is down? Yes

---

(FY 2010) PIA: Secondary Use

---

Will PII data be included with any  
secondary use request?

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 2010) PIA: Program Level Questions

---

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

No

If Yes, Please Specify:

---

Explain how collected data are limited to required elements:

Answer: The heterogeneous and dynamic nature of data collection methods for the myriad of systems covered by the VAMCWB LAN precludes limiting data collection to specific elements.

---

How is data checked for completeness?

Answer: Individual business process owners check the data for completeness as they enter and utilize the data.

---

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

Answer: Currency of data is the responsibility of the end user and the business process owner. There is no centralized or consistent method of validating patient information that is stored within the VAMCWB LAN.

---

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

Answer: Data relevance and accuracy is the sole responsibility of the end user and the business process owner or researcher. There is no centralized or consistent method of verifying patient information stored within the VAMCWB LAN.

---

*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: 75 years after the last episode of patient care. Clinical information is retained in accordance with VA Records Control Schedule 10-1. Demographic information is updated as applications for care are submitted and retained in accordance with VA Records Control Schedule 10-1.

---

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

Answer: In accordance with VA Records Control Schedule 10-1.

---

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 XLIII, 2.b. (Page 190). At the present time, VistA Imaging retains all images.

---

Where are these procedures documented?

Answer: VA Handbook 6300; Record Control Schedule 10-1. In addition Data elimination procedures are documented in the case of employee termination of service. Documented in IM-034 Termination of Computer Access, all data stored by an individual on the Storage Area Network (SAN) is deleted when they leave VA employment. Whenever a personal computer, server or SAN storage device is removed from service, data removal procedures are documented in the Media Sanitization Procedures portion of policy IM-001.

---

How are data retention procedures enforced?

Answer: VA Records Control Schedule 10-1 (page 8): Records Management Responsibilities The Health Information Resources Service (HIRS) is responsible for developing policies and procedures for effective and efficient 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. Local data retention policies affecting data generated by employees is outlined in IM-034.

---

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: The Dept. of Veterans Affairs Record Control Schedule 10-1 was approved March 31, 2008

---

---

(FY 2010) PIA: Children's Online Privacy Protection Act (COPPA)

---

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

No

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

Answer:

---

## (FY 2010) PIA: Security

---

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured. Yes

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.. Yes

---

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

If 'No' to any of the 3 questions above, please describe why:

Answer:

---

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

If 'No' please describe why:

Answer:

---

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

Answer: We follow NIST and FISMA regulatory guidance.

---

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

Answer: (Other Risks)

---

Explain what security controls are being used to mitigate these risks.

(Check all that apply)

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

Answer: (Other Controls)

---

## PIA: PIA Assessment

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

Answer: 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 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.

---

(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.

Name	Description	Comments
Minor app #1		
<input type="checkbox"/> Is PII collected by this min or application?		
<input type="checkbox"/> Does this minor application store PII?		
If yes, where?		
Who has access to this data?		

Name	Description	Comments
Minor app #2		
<input type="checkbox"/> Is PII collected by this min or application?		
<input type="checkbox"/> Does this minor application store PII?		
If yes, where?		
Who has access to this data?		

Name	Description	Comments
Minor app #3		
<input type="checkbox"/> Is PII collected by this min or application?		
<input type="checkbox"/> Does this minor application store PII?		
If yes, where?		
Who has access to this data?		

## (FY 2010) PIA: Final Signatures

Facility Name: VA Medical Center, Wilkes-Barre, PA

Title:	Name:	Phone:	Email:
Privacy Officer:	Sharon Czuk	570-821-3521x4925	sharon.czuk2@va.gov
Information Security Officer:	Edward Wademan	570-821-3521x7726	edward.wademan@va.gov
Chief Information Officer:	David Longmore	570-821-7286	david.longmore@va.gov
Person Completing Document:	Edward Wademan	570-821-3521x7726	edward.wademan@va.gov
System / Application / Program Manager:	David Longmore (For Jack Galvin)	518-626-6244	jack.galvin@va.gov

Date of Report:

12/1/2009

OMB Unique Project Identifier

029-00-02-00-01-1120-00-404-143

Project Name

Region 4>VHA>VISN 04>Wilkes-barre HCS>LAN