

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

### **Roles and Responsibilities:**

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

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

**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>Clarksburg VAMC>VistA-  
  VMS

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

The Clarksburg VistA Legacy system a Major Application and is the software platform on which the VHA healthcare facilities operate their software applications and support for E-government initiatives. Approximately 1134 employees, students, and contractors utilize the system. VistA 4 has migrated all hardware and data maintenance to the Northeast Regional Data Center in Philadelphia, PA. Clarksburg maintains a shadow server for a up to the minute Read Only copy of VistA for contingency purposes. VistA links the facility computer network to over 100 applications and databases across the nation. VistA supports the Clarksburg VAMC, 4 Community Based Clinics in

Description of System / Application / Program: Wood Co., Tucker Co,

---

Facility Name: Louis A. Johnson Healthcare System (Clarksburg VA)

Title:	Name:	Phone:	Email:
Privacy Officer:	Kimberly Lodge	304-623-3461	<a href="mailto:Kimberly.Lodge@va.gov">Kimberly.Lodge@va.gov</a>

Information Security Officer:	Sharon Krichbaum	304-623-3461	<a href="mailto:Sharon.Krichbaum@va.gov">Sharon.Krichbaum@va.gov</a>
Chief Information Officer:	Wendell Sherman	304-626-7025	<a href="mailto:Wendell.Sherman@va.gov">Wendell.Sherman@va.gov</a>
Person Completing Document:	Sharon Krichbaum	304-623-3461	<a href="mailto:Sharon.Krichbaum@va.gov">Sharon.Krichbaum@va.gov</a>
Other Titles:			

Other Titles:

Other Titles:

Date of Last PIA Approved by VACO Privacy

Services: (MM/YYYY) 01/2008

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: FY09 20,684 veterans served

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. 24 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): 11/2009

**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?

- 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

2. Name of the System of Records:

VistA-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?

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?

No

Provided at

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.

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)	Paper & Electronic	Healthcare	Verbal & Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Benefits, Healthcare	Verbal & Written	Written
Service Information	ALL	Benefits, Healthcare	Verbal & Written	Written
Medical Information	ALL	Benefits, Healthcare	Verbal & Written	Written
Criminal Record Information	ALL	Healthcare	Verbal & Written	Written
Guardian Information	ALL	Benefits, Healthcare	Verbal & Written	Written
Education Information	ALL	Benefits, Healthcare	Verbal & Written	Written
Benefit Information	ALL	Benefits, Healthcare	Verbal & Written	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)	Yes	Veteran	Voluntary	On the form
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	On the form
Service Information	Yes	Veteran	Voluntary	On the form
Medical Information	Yes	Veteran	Voluntary	On the form
Criminal Record Information	No			
Guardian Information	Yes	Veteran	Voluntary	On the form
Education Information	Yes	VA Files / Databases (Identify file)	Voluntary	ON the form
Benefit Information	Yes	Veteran	Voluntary	On the form
Other (Explain)				
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, other VAMC	Yes	Healthcare, Benefits	Both PII & PHI	HIPAA
Other Veteran Organization	DoD	No	Healthcare, Benefits	Both PII & PHI	MOU
Other Federal Government Agency	CDC, Cancer Registry	No	Healthcare	Both PII & PHI	MOU, Standing letters, DUA
State Government Agency	Sate Health Dept., Cancer Registry	No	Healthcare	Both PII & PHI	MOU, Standing letters, DUA
Local Government Agency					
Research Entity	WVU Research	No	deidentified Healthcare	N/A	Signed consent
Other Project / System		No			
Other Project / System		No			
Other Project / System		No			

(FY 2010) PIA: Access to Records

Does the system gather information from another system? No  
 Please enter the name of the system:

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 Yes

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? Yes

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

---

Describe process for authorizing access  
to this data.

Answer: special consent form

---

**(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: Data is collected electronically based on t

---

How is data checked for completeness?  
Answer: Data is reviewed by staff and compared to

---

What steps or procedures are taken to ensure the data remains current and not out of date?  
Answer: Clinical data is not removed. Administrati

---

How is new data verified for relevance, authenticity and accuracy?  
Answer: New data is compared with printed form

---

*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: Electronic final version of patient medical

---

Explain why the information is needed for the indicated retention period?  
Answer: To comply with Federal Regulations, RCS :

---

What are the procedures for eliminating data at the end of the retention period?  
Answer: Electronic Final Version of Patient Medica

---

Where are these procedures documented?  
Answer: VA Handbook 6300 and RCS 10-1

---

How are data retention procedures enforced?  
Answer: Records Officer is responsible for develop

---

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 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: Certification & Accreditation 2008 with an Authority to Operate awarded. Contin

---

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 type="checkbox"/> Blackmail                                       | <input checked="" type="checkbox"/> Computer Misuse                       |
| <input 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 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 type="checkbox"/> Vandalism/Rioting                                |
| <input type="checkbox"/> Denial of Service Attacks                       | <input checked="" type="checkbox"/> Errors (Configuration and Data Entry) |
| <input 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 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: Review of risk assessment and security controls, privacy and consent

---

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: VBA Minor Applications

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

Records Locator System	Education Training Website	Appraisal System
Veterans Assistance Discharge System (VADS)	VR&E Training Website	Web Electronic Lender Identification
LGY Processing	VA Reserve Educational Assistance Program	CONDO PUD Builder
Loan Service and Claims	Web Automated Verification of Enrollment	Centralized Property Tracking System
LGY Home Loans	Right Now Web	Electronic Appraisal System
Search Participant Profile (SPP)	VA Online Certification of Enrollment (VA-ONCE)	Web LGY
Control of Veterans Records (COVERS)	Automated Folder Processing System (AFPS)	Access Manager
SHARE	Personal Computer Generated Letters (PCGL)	SAHSHA
Modern Awards Process Development (MAP-D)	Personnel Information Exchange System (PIES)	VBA Data Warehouse
Rating Board Automation 2000 (RBA2000)	Rating Board Automation 2000 (RBA2000)	Distribution of Operational Resources (DOOR)
State of Case/Supplemental (SOC/SSOC)	SHARE	Enterprise Wireless Messaging System (Blackberry)
Awards	State Benefits Reference System	VBA Enterprise Messaging System
Financial and Accounting System (FAS)	Training and Performance Support System (TPSS)	LGY Centralized Fax System
Eligibility Verification Report (EVR)	Veterans Appeals Control and Locator System (VACOLS)	Review of Quality (ROQ)
Automated Medical Information System (AMIS)290	Veterans On-Line Applications (VONAPP)	Automated Sales Reporting (ASR)
Web Automated Reference Material System (WARMS)	Automated Medical Information Exchange II (AIME II)	Electronic Card System (ECS)
Automated Standardized Performance Elements Nationwide (ASPEN)	Committee on Waivers and Compromises (COWC)	Electronic Payroll Deduction (EPD)
Inquiry Routing Information System (IRIS)	Common Security User Manager (CSUM)	Financial Management Information System (FMI)
National Silent Monitoring (NSM)	Compensation and Pension (C&P) Record Interchange (CAPRI)	Purchase Order Management System (POMS)
Web Service Medical Records (WebSMR)	Control of Veterans Records (COVERS)	Veterans Canteen Web
Systematic Technical Accuracy Review (STAR)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)	Inventory Management System (IMS)
Fiduciary STAR Case Review	Fiduciary Beneficiary System (FBS)	Synquest
Veterans Exam Request Info System (VERIS)	Hearing Officer Letters and Reports System (HOLAR)	RAI/MDS
Web Automated Folder Processing System (WAFPS)	Inforce	ASSISTS
Courseware Delivery System (CDS)	Awards	MUSE
Electronic Performance Support System (EPSS)	Actuarial	Bbraun (CP Hemo)
Veterans Service Representative (VSR) Advisor	Insurance Self Service	VIC
Loan Guaranty Training Website	Insurance Unclaimed Liabilities	BCMA Contingency Machines
C&P Training Website	Insurance Online	Script Pro

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.

Minor app #1	Name		Description	Comments
			Is PII collected by this min or application?	
			Does this minor application store PII?	
			If yes, where?	
		Who has access to this data?		

Minor app #2	Name		Description	Comments
			Is PII collected by this min or application?	
			Does this minor application store PII?	
			If yes, where?	
		Who has access to this data?		

Minor app #3	Name		Description	Comments
			Is PII collected by this min or application?	
			Does this minor application store PII?	
			If yes, where?	
		Who has access to this data?		

---

Baker System	Veterans Assistance Discharge System (VADS)
Dental Records Manager	VBA Training Academy
Sidexis	Veterans Service Network (VETSNET)
Priv Plus	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
Mental Health Assistant	BIRLS
Telecare Record Manager	Centralized Accounts Receivable System (CARS)
Omnicell	Compensation & Pension (C&P)
Powerscribe Dictation System	Corporate Database
EndoSoft	Control of Veterans Records (COVERS)
Compensation and Pension (C&P)	Data Warehouse
Montgomery GI Bill	INS - BIRLS
Vocational Rehabilitation & Employment (VR&E) CH 31	Mobilization
Post Vietnam Era educational Program (VEAP) CH 32	Master Veterans Record (MVR)
Spinal Bifida Program Ch 18	BDN Payment History
C&P Payment System	
Survivors and Dependents Education Assistance CH 35	
Reinstatement Entitlement Program for Survivors (REAPS)	
Educational Assistance for Members of the Selected Reserve Program CH 1606	
Reserve Educational Assistance Program CH 1607	
Compensation & Pension Training Website	
Web-Enabled Approval Management System (WEAMS)	
FOCAS	
Work Study Management System (WSMS)	
Benefits Delivery Network (BDN)	
Personnel and Accounting Integrated Data and Fee Basis (PAID)	
Personnel Information Exchange System (PIES)	
Rating Board Automation 2000 (RBA2000)	
SHARE	
Service Member Records Tracking System	

(FY 2010) PIA: VISTA Minor Applications

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

X	ACCOUNTS RECEIVABLE	X	DRUG ACCOUNTABILITY	X	INPATIENT MEDICATIONS	X
	ADP PLANNING (PLANMAN)	X	DSS EXTRACTS	X	INTAKE/OUTPUT	X
X	ADVERSE REACTION TRACKING	X	EDUCATION TRACKING	X	INTEGRATED BILLING	X
X	ASISTS	X	EEO COMPLAINT TRACKING	X	INTEGRATED PATIENT FUNDS	X
X	AUTHORIZATION/SUBSCRIPTION	X	ELECTRONIC SIGNATURE	X	INTERIM MANAGEMENT SUPPORT	X
X	AUTO REPLENISHMENT/WARD STOCK	X	ENGINEERING	X	KERNEL	X
X	AUTOMATED INFO COLLECTION SYS	X	ENROLLMENT APPLICATION SYSTEM	X	KIDS	X
X	AUTOMATED LAB INSTRUMENTS	X	EQUIPMENT/TURN-IN REQUEST	X	LAB SERVICE	X
X	AUTOMATED MED INFO EXCHANGE	X	EVENT CAPTURE	X	LETTERMAN	X
X	BAR CODE MED ADMIN	X	EVENT DRIVEN REPORTING	X	LEXICON UTILITY	X
X	BED CONTROL		EXTENSIBLE EDITOR	X	LIBRARY	
X	BENEFICIARY TRAVEL		EXTERNAL PEER REVIEW	X	LIST MANAGER	X
X	CAPACITY MANAGEMENT - RUM	X	FEE BASIS	X	MAILMAN	X
	CAPRI	X	FUNCTIONAL INDEPENDENCE	X	MASTER PATIENT INDEX VISTA	X
X	CAPACITY MANAGEMENT TOOLS	X	GEN. MED. REC. - GENERATOR	X	MCCR NATIONAL DATABASE	X
X	CARE MANAGEMENT	X	GEN. MED. REC. - I/O	X	MEDICINE	X
X	CLINICAL CASE REGISTRIES	X	GEN. MED. REC. - VITALS	X	MENTAL HEALTH	X
X	CLINICAL INFO RESOURCE NETWORK	X	GENERIC CODE SHEET		MICOM	
X	CLINICAL MONITORING SYSTEM		GRECC	X	MINIMAL PATIENT DATASET	X
X	CLINICAL PROCEDURES	X	HEALTH DATA & INFORMATICS	X	MYHEALTHEVET	X
X	CLINICAL REMINDERS	X	HEALTH LEVEL SEVEN	X	Missing Patient Reg (Original) A4EL	X
X	CMOP	X	HEALTH SUMMARY	X	NATIONAL DRUG FILE	X
X	CONSULT/REQUEST TRACKING	X	HINQ	X	NATIONAL LABORATORY TEST	X
X	CONTROLLED SUBSTANCES	X	HOSPITAL BASED HOME CARE	X	NDBI	X
X	CPT/HCPCS CODES	X	ICR - IMMUNOLOGY CASE REGISTRY	X	NETWORK HEALTH EXCHANGE	X
	CREDENTIALS TRACKING	X	IFCAP		NOIS	X
X	DENTAL	X	IMAGING	X	NURSING SERVICE	X
X	DIETETICS	X	INCIDENT REPORTING	X	OCCURRENCE SCREEN	X
X	DISCHARGE SUMMARY	X	INCOME VERIFICATION MATCH	X	ONCOLOGY	
X	DRG GROUPER	X	INCOMPLETE RECORDS TRACKING	X	ORDER ENTRY/RESULTS REPORTING	X

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
Vista WEB	VA medical records from other facilities accessed via web access.	
<input type="checkbox"/> NO Is PII collected by this min or application?		
<input type="checkbox"/> NO Does this minor application store PII?		
<input type="checkbox"/> If yes, where?		
<input type="checkbox"/> Who has access to this data?		
<input type="checkbox"/> Authorized VA employees		

Minor app #1

Name	Description	Comments
<input type="checkbox"/> NO Is PII collected by this min or application?		
<input type="checkbox"/> Does this minor application store PII?		
<input type="checkbox"/> If yes, where?		
<input type="checkbox"/> Who has access to this data?		

Minor app #2

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

Minor app #3

---

OUTPATIENT PHARMACY	X	SOCIAL WORK
PAID	X	SPINAL CORD DYSFUNCTION
PATCH MODULE	X	SURGERY
PATIENT DATA EXCHANGE	X	SURVEY GENERATOR
PATIENT FEEDBACK	X	TEXT INTEGRATION UTILITIES
PATIENT REPRESENTATIVE	X	TOOLKIT
PCE PATIENT CARE ENCOUNTER	X	UNWINDER
PCE PATIENT/IHS SUBSET	X	UTILIZATION MANAGEMENT ROLLUP
PHARMACY BENEFITS MANAGEMENT		UTILIZATION REVIEW
PHARMACY DATA MANAGEMENT	X	VA CERTIFIED COMPONENTS - DSSI
PHARMACY NATIONAL DATABASE	X	VA FILEMAN
PHARMACY PRESCRIPTION PRACTICE	X	VBECs
POLICE & SECURITY	X	VDEF
PROBLEM LIST	X	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES		VHS&RA ADP TRACKING SYSTEM
PROSTHETICS	X	VISIT TRACKING
QUALITY ASSURANCE INTEGRATION	X	VISTALINK
QUALITY IMPROVEMENT CHECKLIST	X	VISTALINK SECURITY
QUASAR	X	VISUAL IMPAIRMENT SERVICE TEAM ANRV
RADIOLOGY/NUCLEAR MEDICINE	X	VOLUNTARY TIMEKEEPING
RECORD TRACKING		VOLUNTARY TIMEKEEPING NATIONAL
REGISTRATION	X	WOMEN'S HEALTH
RELEASE OF INFORMATION - DSSI		CARE TRACKER
REMOTE ORDER/ENTRY SYSTEM		
RPC BROKER		
RUN TIME LIBRARY		
SAGG		
SCHEDULING		
SECURITY SUITE UTILITY PACK		
SHIFT CHANGE HANDOFF TOOL		

(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
		<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?			

Minor app #2	Name		Description		Comments
		<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?			

Minor app #3	Name		Description		Comments
		<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: Louis A. Johnson Healthcare System (Clarksburg VA)

Title:	Name:	Phone:	Email:
Privacy Officer:	Kimberly Lodge	304-623-3461	Kimberly.Lodge@va.gov
Digital Signature Block			
Information Security Officer:	Sharon Krichbaum	304-623-3461	Sharon.Krichbaum@va.gov
Digital Signature Block			
Chief Information Officer:	Wendell Sherman	304-626-7025	Wendell.Sherman@va.gov
Digital Signature Block			
Person Completing Document:	Sharon Krichbaum	304-623-3461	Sharon.Krichbaum@va.gov
Digital Signature Block			
System / Application / Program Manager:		0	0
Digital Signature Block			

Date of Report: 11/1/2009  
 OMB Unique Project Identifier: 029-00-01-11-01-1180-00

Project Name: Region 4>VHA>VISN 04>Clarksburg  
 VAMC>VistA-VMS