

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

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 1>WRJ>LAN

OMB Unique System / Application / Program

Identifier (AKA: UPID #): IT Infrastructure 029-00-02-00-01-1120-00

The LAN system is the hardware infrastructure on which the VHA health care facilities operate their software applications and support for E-Government initiatives, also known as a General Support System. It includes the computer equipment associated with clinical operations and the employees (approximately 750 FTE) necessary to operate the system. The White River Junction LAN system supports IT services across the VAMC facility and the community based outpatient clinics in VT and Northern New Hampshire. The LAN provides critical connectivity that supports the delivery of healthcare to veterans and their dependants. Using the LAN, the VA health care provider can access applications and meet a wide range of health care data needs. The LAN system is in the mature phase of the capital investment lifecycle.

Description of System / Application / Program: mature phase of the capital investment lifecycle.

Facility Name: White River Junction, VT VAMC (#405)

Title:	Name:	Phone:	Email:
Privacy Officer:	Hallmartel, Clarence I.	802-295-9363 x5748	clarence.hallmartel@va.gov
Information Security Officer:	DeBlock, Michael S.	802-296-6306	michael.deblock@va.gov
Chief Information Officer:	Rafus, Matthew	802-295-9363 x6288	matthew.rafus@va.gov
Person Completing Document:	DeBlock, Michael S.	802-296-6306	michael.deblock@va.gov
Other Titles:			

Other Titles:

Other Titles:

Date of Last PIA Approved by VACO Privacy

Services: (MM/YYYY) 07/2008

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:

86575 unique records in VistA.

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.

Operational since 1998, approximately 11 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?
- 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):

02VA135; 04VA115; 07VA138; 14VA135; 20VA138; 23VA163; 24VA19; 28VA119;
29VA11; 32VA00; 33VA113; 34VA12; 54VA17; 57VA10C2; 64VA15; 65VA122;
69VA131; 73VA14; 77VA10Q; 79VA19; 84VA111K; 89VA19; 90VA194;
91VA111C; 93VA131; 97VA105; 98VA104A; 99VA131; 100VA10NS10; 105VA131;
106VA17; 108VA11S; 110VA10; 113VA112; 114VA16; 115VA10; 117VA103;
121VA19; 130VA19

Applicants for Employment under Title 38, USC-VA; Blood Donor Information-VA;
Department of Medicine and Surgery Engineering Employee Management Information
Records-VA; Individuals Serving on a Fee Basis or without Compensation (Consultants,
Attendings, Others) Personnel Records-VA; Motor Vehicle Operator Accident Records-
VA; Non-VA Fee Basis Records-VA; Patient Medical Records-VA; Personnel
Registration under Controlled Substance Act-VA; Physician, Dentist and Supervisory
Nurse Professional Standards Board Action File-VA; Veteran, Employee and Citizen
Health Care Facility Investigation Records-VA; National Prosthetics Patient Database-
VA; Veteran, Patient, Employee and Volunteer Research and Development Project
Records-VA; Health Administration Center Civilian Health and Medical program
Records-VA; Voluntary Service Records-VA; Readjustment Counseling Service (RCS)
Vet Center Program-VA; Community Placement Program-VA; Ionizing Radiation
Registry-VA; Health Professional Scholarship Program-VA; Health Care Provider
Credentialing and Privileging Records-VA; Veterans Health Information System and
Technology Architecture (VISTA)-VA; National Chaplain Management Information
System (NCMIS); Health Eligibility Records-VA; Call Detail Records-VA; Homeless
Providers Grant & Per Diem Program Records-VA; Gulf War Registry-VA;

2. Name of the System of Records:

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?	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.

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)	ALL	Clinical and administrative information will be used in the effort to treat and contact the veteran.	All	All
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Clinical and administrative information will be used in the effort to treat and contact the veteran.	All	All
Service Information	ALL	Clinical and administrative information will be used in the effort to treat and contact the veteran.	All	All
Medical Information	ALL	Clinical and administrative information will be used in the effort to treat and contact the veteran.	All	All
Criminal Record Information	ALL	Clinical and administrative information will be used in the effort to treat and contact the veteran.	All	All
Guardian Information	ALL	Clinical and administrative information will be used in the effort to treat and contact the veteran.	All	All
Education Information	ALL	Clinical and administrative information will be used in the effort to treat and contact the veteran.	All	All
Benefit Information	ALL	Clinical and administrative information will be used in the effort to treat and contact the veteran.	All	All
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	Other (Explain)	Mandatory	Source is all of the above.

Family Relation (spouse, children, parents, grandparents, etc)	Yes	Other (Explain)	Mandatory	Source is all of the above.
Service Information	Yes	Other (Explain)	Mandatory	Source is all of the above.
Medical Information	Yes	Other (Explain)	Mandatory	Source is all of the above.
Criminal Record Information	Yes	Other (Explain)	Mandatory	Source is all of the above.
Guardian Information	Yes	Other (Explain)	Mandatory	Source is all of the above.
Education Information	Yes	Other (Explain)	Mandatory	Source is all of the above.
Benefit Information	Yes	Other (Explain)	Mandatory	Source is all of the above.
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	Yes	VA internally shares clinical and administrative data with the VBA for the purpose of ensuring benefits are received.	Both PII & PHI	Privacy Act / VA Handbook 1605.1
Other Veteran Organization	VSO's	Yes	VSO (PVA, WWII Vets, VFW, DVA): are allowed to assist veterans with their benefits only after proper authorization is granted by the veteran.	Both PII & PHI	Privacy Act / VA Handbook 1605.1
Other Federal Government Agency	CDC	Yes	VA internally shares clinical and administrative data with the CDC in an effort to protect the public communities.	Both PII & PHI	Privacy Act / VA Handbook 1605.1
State Government Agency	State Soldier's Home	Yes	State soldiers homes to provide care.	Both PII & PHI	Privacy Act / VA Handbook 1605.1
Local Government Agency		No			
Research Entity		No			
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

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?

Yes

Drug/Alcohol Counseling Mental Health HIV

if yes, please check all that apply:

Research Sickle Cell Other (Please Explain)

Describe process for authorizing access to this data.

Answer: IRB and R&D approval for any research projects that will reference PII or PHI.

(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 the automation of VA forms and clinical procedures.

How is data checked for completeness?

Answer: Data is reviewed by staff and compared to paper forms.

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

Answer: Clinical data is not removed. Administrative data is updated with each application for care.

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

Answer: New data is compared with printed form or via patient verification.

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.

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: To remain in compliance with RCS 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. We are performing a study to explore whether some images can be eliminated on an earlier schedule.

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 (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. Disposition of Records

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: At the Department level, the CIO's Office of Cyber & Information Security (OCIS) is responsible for the establishment of directives, policies, & procedures which are consistent with the provisions of Federal Information Security Management Act (FISMA) as well as guidance issued by the Office of Management & Budget (OMB), the National Institute of Standards & Technology (NIST), & other requirements that LAN is and has been subject to. In addition, OCIS administers and manages Department-wide security solutions, such as anti-virus protection, authentication, vulnerability scanning & penetration testing, & intrusion detection systems, and incident response (800-61). At the LAN project level -The Project Manager ensures that CIO-provided security directives are integrated into the project's security plan & implemented by VA & contractor staff throughout the project funding needs are dependent on IT security requirements identified in the system development life cycle (800-64) (i.e. risk assessments (800-30), certification and accreditation (800-37 and 800-53)), as well as identified security weaknesses that must be corrected. Minimum security controls for a high system are operational in accordance with NIST 800-53 guidelines

Explain what security risks were identified in the security assessment? (Check all that apply)

- Air Conditioning Failure
- Chemical/Biological Contamination
- Blackmail
- Bomb Threats
- Cold/Frost/Snow
- Communications Loss
- Computer Intrusion
- Data Destruction
- Data Disclosure
- Data Integrity Loss
- Denial of Service Attacks
- Earthquakes
- Eavesdropping/Interception
- Fire (False Alarm, Major, and Minor)
- Flooding/Water Damage
- Hardware Failure
- Malicious Code
- Computer Misuse
- Power Loss
- Sabotage/Terrorism
- Storms/Hurricanes
- Substance Abuse
- Theft of Assets
- Theft of Data
- Vandalism/Rioting
- Errors (Configuration and Data Entry)
- Burglary/Break In/Robbery
- Identity Theft
- Fraud/Embezzlement

Answer: (Other Risks)

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

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

the loss of availability could be expected to have a serious 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.

Answer: (Other Controls)

The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

PIA: PIA Assessment

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

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.

Answer: The LAN is an ongoing project and is governed by existing policies and procedures.

The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.

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 **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

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

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)

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 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	Baker System	Veterans Assistance Discharge System (VADS)
Veterans Assistance Discharge System (VADS)	VR&E Training Website	Web Electronic Lender Identification	Dental Records Manager	VBA Training Academy
LGY Processing	VA Reserve Educational Assistance Program	CONDO PUD Builder	Sidexis	Veterans Service Network (VETSNET)
Loan Service and Claims	Web Automated Verification of Enrollment	Centralized Property Tracking System	Priv Plus	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
LGY Home Loans	Right Now Web	Electronic Appraisal System	Mental Health Assistant	BIRLS
Search Participant Profile (SPP)	VA Online Certification of Enrollment (VA-ONCE)	Web LGY	Telecare Record Manager	Centralized Accounts Receivable System (CARS)
Control of Veterans Records (COVERS)	Automated Folder Processing System (AFPS)	Access Manager	OmniceII	Compensation & Pension (C&P)
SHARE	Personal Computer Generated Letters (PCGL)	SAHSHA	Powerscribe Dictation System	Corporate Database
Modern Awards Process Development (MAP-D)	Personnel Information Exchange System (PIES)	VBA Data Warehouse	EndoSoft	Control of Veterans Records (COVERS)
Rating Board Automation 2000 (RBA2000)	Rating Board Automation 2000 (RBA2000)	Distribution of Operational Resources (DOOR)	Compensation and Pension (C&P)	Data Warehouse
State of Case/Supplemental (SOC/SSOC)	SHARE	Enterprise Wireless Messaging System (Blackberry)	Montgomery GI Bill	INS - BIRLS
Awards	State Benefits Reference System	VBA Enterprise Messaging System	Vocational Rehabilitation & Employment (VR&E) CH 31	Mobilization
Financial and Accounting System (FAS)	Training and Performance Support System (TPSS)	LGY Centralized Fax System	Post Vietnam Era educational Program (VEAP) CH 32	Master Veterans Record (MVR)
Eligibility Verification Report (EVR)	Veterans Appeals Control and Locator System (VACOLS)	Review of Quality (ROQ)	Spinal Bifida Program Ch 18	BDN Payment History
Automated Medical Information System (AMIS)290	Veterans On-Line Applications (VONAPP)	Automated Sales Reporting (ASR)	C&P Payment System	
Web Automated Reference Material System (WARMS)	Automated Medical Information Exchange II (AIME II)	Electronic Card System (ECS)	Survivors and Dependents Education Assistance CH 35	
Automated Standardized Performance Elements Nationwide (ASPEN)	Committee on Waivers and Compromises (COWC)	Electronic Payroll Deduction (EPD)	Reinstatement Entitlement Program for Survivors (REAPS)	
Inquiry Routing Information System (IRIS)	Common Security User Manager (CSUM)	Financial Management Information System (FMI)	Educational Assistance for Members of the Selected Reserve Program CH 1606	
National Silent Monitoring (NSM)	Compensation and Pension (C&P) Record Interchange (CAPRI)	Purchase Order Management System (POMS)	Reserve Educational Assistance Program CH 1607	
Web Service Medical Records (WebSMR)	Control of Veterans Records (COVERS)	Veterans Canteen Web	Compensation & Pension Training Website	
Systematic Technical Accuracy Review (STAR)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)	Inventory Management System (IMS)	Web-Enabled Approval Management System (WEAMS)	
Fiduciary STAR Case Review	Fiduciary Beneficiary System (FBS)	Synquest	FOCAS	
Veterans Exam Request Info System (VERIS)	Hearing Officer Letters and Reports System (HOLAR)	RAI/MDS	Work Study Management System (WSMS)	
Web Automated Folder Processing System (WAFPS)	Inforce	ASSISTS	Benefits Delivery Network (BDN)	
Courseware Delivery System (CDS)	Awards	MUSE	Personnel and Accounting Integrated Data and Fee Basis (PAID)	
Electronic Performance Support System (EPSS)	Actuarial	Bbraun (CP Hemo)	Personnel Information Exchange System (PIES)	
Veterans Service Representative (VSR) Advisor	Insurance Self Service	VIC	Rating Board Automation 2000 (RBA2000)	
Loan Guaranty Training Website	Insurance Unclaimed Liabilities	BCMA Contingency Machines	SHARE	
C&P Training Website	Insurance Online	Script Pro	Service Member Records Tracking System	

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
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 #1

Name	Description	Comments
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
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

(FY 2010) PIA: VISTA Minor Applications

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

ACCOUNTS RECEIVABLE	DRUG ACCOUNTABILITY	INPATIENT MEDICATIONS	OUTPATIENT PHARMACY	SOCIAL WORK
ADP PLANNING (PLANMAN)	DSS EXTRACTS	INTAKE/OUTPUT	PAID	SPINAL CORD DYSFUNCTION SURGERY
ADVERSE REACTION TRACKING ASISTS	EDUCATION TRACKING	INTEGRATED BILLING	PATCH MODULE	SURVEY GENERATOR
	EEO COMPLAINT TRACKING	INTEGRATED PATIENT FUNDS	PATIENT DATA EXCHANGE	
AUTHORIZATION/SUBSCRIPTION	ELECTRONIC SIGNATURE	INTERIM MANAGEMENT SUPPORT	PATIENT FEEDBACK	TEXT INTEGRATION UTILITIES
AUTO REPLENISHMENT/WARD STOCK	ENGINEERING	KERNEL	PATIENT REPRESENTATIVE	TOOLKIT
AUTOMATED INFO COLLECTION SYS	ENROLLMENT APPLICATION SYSTEM	KIDS	PCE PATIENT CARE ENCOUNTER	UNWINDER
AUTOMATED LAB INSTRUMENTS	EQUIPMENT/TURN-IN REQUEST	LAB SERVICE	PCE PATIENT/IHS SUBSET	UTILIZATION MANAGEMENT ROLLUP
AUTOMATED MED INFO EXCHANGE	EVENT CAPTURE	LETTERMAN	PHARMACY BENEFITS MANAGEMENT	UTILIZATION REVIEW
BAR CODE MED ADMIN	EVENT DRIVEN REPORTING	LEXICON UTILITY	PHARMACY DATA MANAGEMENT	VA CERTIFIED COMPONENTS - DSSI
BED CONTROL	EXTENSIBLE EDITOR	LIBRARY	PHARMACY NATIONAL DATABASE	VA FILEMAN
BENEFICIARY TRAVEL	EXTERNAL PEER REVIEW	LIST MANAGER	PHARMACY PRESCRIPTION PRACTICE	VBECS
CAPACITY MANAGEMENT - RUM	FEE BASIS	MAILMAN	POLICE & SECURITY	VDEF
CAPRI	FUNCTIONAL INDEPENDENCE	MASTER PATIENT INDEX VISTA	PROBLEM LIST	VENDOR - DOCUMENT STORAGE SYS
CAPACITY MANAGEMENT TOOLS	GEN. MED. REC. - GENERATOR	MCCR NATIONAL DATABASE	PROGRESS NOTES	VHS&RA ADP TRACKING SYSTEM
CARE MANAGEMENT	GEN. MED. REC. - I/O	MEDICINE	PROSTHETICS	VISIT TRACKING
CLINICAL CASE REGISTRIES	GEN. MED. REC. - VITALS	MENTAL HEALTH	QUALITY ASSURANCE INTEGRATION	VISTALINK
CLINICAL INFO RESOURCE NETWORK	GENERIC CODE SHEET	MICOM	QUALITY IMPROVEMENT CHECKLIST	VISTALINK SECURITY
CLINICAL MONITORING SYSTEM	GRECC	MINIMAL PATIENT DATASET	QUASAR	VISUAL IMPAIRMENT SERVICE TEAM ANRV
CLINICAL PROCEDURES	HEALTH DATA & INFORMATICS	MYHEALTHVET	RADIOLOGY/NUCLEAR MEDICINE	VOLUNTARY TIMEKEEPING
CLINICAL REMINDERS	HEALTH LEVEL SEVEN	Missing Patient Reg (Original)	RECORD TRACKING	VOLUNTARY TIMEKEEPING NATIONAL
CMOP	HEALTH SUMMARY	A4EL	REGISTRATION	WOMEN'S HEALTH
CONSULT/REQUEST TRACKING	HINQ	NATIONAL LABORATORY TEST	RELEASE OF INFORMATION - DSSI	CARE TRACKER
CONTROLLED SUBSTANCES	HOSPITAL BASED HOME CARE	NDBI	REMOTE ORDER/ENTRY SYSTEM	
CPT/HCP/CS CODES	ICR - IMMUNOLOGY CASE REGISTRY	NETWORK HEALTH EXCHANGE	RPC BROKER	
CREDENTIALS TRACKING	IFCAP	NOIS	RUN TIME LIBRARY	
DENTAL	IMAGING	NURSING SERVICE	SAGG	
DIETETICS	INCIDENT REPORTING	OCCURRENCE SCREEN	SCHEDULING	
DISCHARGE SUMMARY	INCOME VERIFICATION MATCH	ONCOLOGY	SECURITY SUITE UTILITY PACK	
DRG GROUPER	INCOMPLETE RECORDS TRACKING	ORDER ENTRY/RESULTS REPORTING	SHIFT CHANGE HANDOFF TOOL	

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

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

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

(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: White River Junction, VT VAMC (#405)

Title:	Name:	Phone:	Email:
Privacy Officer:	Hallmartel, Clarence I.	802-295-9363 x5748	clarence.hallmartel@va.gov
Digital Signature Block			
Information Security Officer:	DeBlock, Michael S.	802-296-6306	michael.deblock@va.gov
Digital Signature Block			
Chief Information Officer:	Rafus, Matthew	802-295-9363 x6288	matthew.rafus@va.gov
Digital Signature Block			
Person Completing Document:	DeBlock, Michael S.	802-296-6306	michael.deblock@va.gov
Digital Signature Block			
System / Application / Program Manager:		0	0
Digital Signature Block			

Date of Report:

11/9/2009

OMB Unique Project Identifier

IT Infrastructure 029-00-02-00-01-1120-00

Project Name

Region 4>VHA>VISN 1>WRJ>LAN