

Welcome to the PIA for FY 2011!



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.

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

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 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 Directive 6508.
- 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 Directive 6508 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

Microsoft Office 2003: 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.

Microsoft Office 2007: To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable

All Macros; 2) Click OK

Final Signatures

Final Signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.



Privacy Impact Assessment Uploaded into SMART

Privacy Impact Assessments should be uploaded into C&A section of SMART.

All PIA Validation Letters should be emailed to christina.pettit@va.gov to received full credit for submission.

(FY 2011) PIA: System Identification



Program or System Name: REGION 4 > VHA > VISN 01 > Manchester VAMC > LAN
 OMB Unique System / Application / Program Identifier (AKA: UPID #):
 Description of System/ Application/ Program: The LAN system is the hardware infrastructure on which the applications and support for E-Government initiatives, also computer equipment associated with clinical operations operate the system. The VAMC Manchester LAN system supports community based outpatient clinics in Portsmouth, Somers Center in Auburn, and the Manchester Vet Center located at that supports the delivery of healthcare to veterans and the provider can access applications and meet a wide range of phase of the capital investment lifecycle.

Facility Name: Manchester VAMC

Title:	Name:	Phone:
Privacy Officer:	Shirley S. Martin	(603) 624-4366, ext. 6700
Information Security Officer:	Mary R. Ballard	(603) 626-6537
System Owner/ Chief Information Officer:	John A. Foote	(603) 624-4366, ext. 6618
Information Owner:	John J. Galvin	(518) 626-6244
Other Titles:		
Person Completing Document:	Shirley S. Martin and Mary R. Ballard	

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: 07/2008

Date Approval To Operate Expires: 08/29/2011



What specific legal authorities authorize this program or system:

What is the expected number of individuals that will have their PII stored in this system:

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

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.

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

If No, please explain:

Has a PIA been completed within the last three years?

Date of Report (MM/YYYY):

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on

- 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 complete TAB 2 & TAB 12. (See Co



029-00-02-00-01-1120-00

The VHA health care facilities operate their software known as a General Support System. It includes the staff and the employees (approximately 647 FTE) necessary to support IT services across the Manchester facility, the Manchester, Swarth, Tilton, and Conway, the Northeast Regional Veterans Affairs Medical Center on Liberty Street. The LAN provides critical connectivity for all VA health care dependants. Using the LAN, the VA health care facilities meet their health care data needs. The LAN system is in the mature

Email:

shirley.martin2@va.gov

mary.ballard@va.gov

john.foote@va.gov

jack.galvin@va.gov

Title 38, United States Code, section 7301

22,347 unique patients in FY 10

Operations/Maintenance

Operational since 1993, approximately 18 years



Yes



Yes

07/2008

on this form.

ees, contractors, or others performing work for
name, unique identifier, symbol, or

Comment for Definition of PII)

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.

Yes

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; 08VA11S; 110VA10; 113VA112; 114VA16; 115VA10; 117VA103; 121VA19; 130VA19

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; Consolidated Data Information System;

3. Location where the specific applicable System of Records Notice may be accessed (include the URL): http://www.rms.oit.va.gov/SOR_Records.asp

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 2011) 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	This information is collected to identify the veteran, schedule treatment and manage the provided care.	All	Verbal & Written
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Next-of-kin and emergency contact information is collected to contact other individuals in case of an emergency.	All	Verbal & Written
Service Information	Paper	This information is collected to assess eligibility for VA healthcare benefits and the type of healthcare needed.	Verbally	Verbal & Written
Medical Information	ALL	This information is collected to diagnose and treat the veteran patient.	Verbal & Written	Verbal & Written
Criminal Record Information	Paper & Electronic	This information is collected in an effort to protect all those utilizing the VA systems.	Verbally	Verbally
Guardian Information	Paper	This information is collected to be used in the notification process and as required for medical decisions.	Verbally	Verbally
Education Information	Paper & Electronic	This information is collected to ensure compliance with confidentiality, integrity and authorization.	Verbal & Automatic	Verbal & Automatic



Benefit Information	Paper & Electronic	This information is collected to assess eligibility for VA healthcare benefits and the type of healthcare needed.	Verbally	Verbal & Written
Other (Explain): Insurance and Employment Information	Paper	This information is collected for use in billing for care.	Verbally	Verbal & Written

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	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Mandatory	
Service Information	Yes	Veteran	Mandatory	
Medical Information	Yes	Veteran	Mandatory	
Criminal Record Information	No	State Agency (Identify)	Mandatory	State Police
Guardian Information	Yes	Veteran	Mandatory	
Education Information	Yes	Public (identify specific entity)	Mandatory	Educational Institution
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	VA Claim File
Other (Explain): Insurance and Employment Information for use in billing for care	Yes	Veteran	Mandatory	
Other (Explain): Other (Explain)				

(FY 2011) 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; General Counsel; Other VAMCs	Yes	CAPRI; VistAWeb; Remote Access; Encrypted Email for use in the determination of eligibility or entitlement to benefits and for the purposes of treatment, payment and health care operations.	Both PII & PHI	VHA Handbook 1605.1
Other Veteran Organization	DAV, American Legion, VFW, VVA, PVA, etc.	No	Paper documents and verbal communications with proper authorization for use in the determination of eligibility or entitlement to benefits and for the purposes of treatment, payment and health care operations.	Both PII & PHI	VHA Handbook 1605.1

Other Federal Government Agency				Paper documents and verbal communications with proper authorization for use in determining eligibility for care, purposes of treatment, in an effort to protect the public communities and for income verification to determine if third party collection is possible.		
	DoD, CDC, IRS, SSA	No			Both PII & PHI	VHA Handbook 1605.1
State Government Agency				Paper and electronic documents with proper authorization for the purposes of treatment, as required by state law and in an effort to protect the public communities.		
	Dept. of Public Health, State Cancer Registries, State Veterans Home	No			Both PII & PHI	VHA Handbook 1605.1
Local Government Agency	None					
Research Entity	None					
Other Project / System						
Other Project / System						
Other Project / System						

(FY 2011) PIA: Access to Records

Does the system gather information from another system?			Yes
Please enter the name of the system:	VBA BDN		
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:	<input type="checkbox"/> Through a Written Request <input checked="" type="checkbox"/> Submitted in Person <input checked="" type="checkbox"/> Online via Electronic Form		
Is there a contingency plan in place to process information when the system is down?			Yes



(FY 2011) PIA: Secondary Use



Will PII data be included with any secondary use request?

Yes

- 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: The facility requires a signed consent by the veteran before access to the data is allowed or furnished.

(FY 2011) 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 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: Clinical information is retained in accordance with VHA Records Control Schedule 10-1.

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

Answer: Demographic information is updated as applications for care are submitted and retained in accordance with VHA Records Control Schedule 10-1.

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

Answer: Electronic Final Version of Health Record is destroyed/deleted 75 years after the last episode of patient care as instructed in VHA Records Control Schedule 10-1, Item XLIII-2, b (page 199). VistA Imaging retains all images.

Where are these procedures documented?

Answer: VA Handbook 6300; VHA Record Control Schedule 10-1.

How are data retention procedures enforced?

Answer: The Central Office Forms, Publications and Records management office is responsible for developing policies and procedures for effective and efficient records management through VHA. In addition, the office acts as the liaison between VHA and NARA on issue pertaining to records management practices and procedures. Records Management 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.

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 2011) 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 2011) 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.

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

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

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

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

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

Answer: Employee performance evaluations are conducted semi-annually.

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

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 Information & Technology (OI&T) 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, the Office of Information Protection & Risk Management (IPRM) 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 level, the Region CIO ensures that 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

Burglary/Break In/Robbery

Cold/Frost/Snow

Data Disclosure

Data Integrity Loss

Denial of Service Attacks

Earthquakes

Eavesdropping/Interception

Hardware Failure

Identity Theft

Malicious Code

Power Loss

Sabotage/Terrorism

Storms/Hurricanes

- Burglary/Break In/Robbery
- Cold/Frost/Snow
- Communications Loss
- Computer Intrusion
- Computer Misuse
- Data Destruction

Answer: (Other Risks)

- Eavesdropping/Interception
- Errors (Configuration and Data Entry)
- Fire (False Alarm, Major, and Minor)
- Flooding/Water Damage
- Fraud/Embezzlement

- Storms/Hurricanes
- Substance Abuse
- Theft of Assets
- Theft of Data
- Vandalism/Rioting

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

Access Control

Audit and Accountability

Awareness and Training

Certification and Accreditation Security Assessments

Configuration Management

Contingency Planning

Identification and Authentication

Incident Response

Media Protection

Personnel Security

Physical and Environmental Protection

Risk Management

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 applicable policies and procedures, reconsideration of collections sources and methods, examination of controls to mitigate misuse of information, verification of consent and privacy notice procedures, and careful examination of security controls.

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 integrity 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 integrity could be expected to have a serious adverse effect on operations, assets or individuals.

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

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

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 2011) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?

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

VBA Data Warehouse	X Telecare Record Manager	Web Automated Folder Processing System (WAFPS)
VBA Training Academy	VBA Enterprise Messaging System	Web Automated Reference Material System (WARMS)
Veterans Canteen Web	Veterans On-Line Applications (VONAPP)	Web Automated Verification of Enrollment
VIC	Veterans Service Network (VETSNET)	Web-Enabled Approval Management System (WEAMS)
VR&E Training Website	Web Electronic Lender Identification	Web Service Medical Records (WebSMR)
Web LGY		Work Study Management System (WSMS)

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?
Does this minor application store PII?
If yes, where?
Who has access to this data?

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?

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?

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

- | | | | |
|---------------|----------------------|-------------------------------|---------------------------------------|
| X ASISTS | X Beneficiary Travel | X Accounts Receivable | X Adverse Reaction Tracking |
| Bed Control | X Care Management | X ADP Planning (PlanMan) | X Authorization/ Subscription |
| X CAPRI | X Care Tracker | X Bad Code Med Admin | X Auto Replenishment/ Ward Stock |
| X CMOP | X Clinical Reminders | X Clinical Case Registries | X Automated Info Collection Sys |
| X Dental | X CPT/ HCPCS Codes | X Clinical Procedures | X Automated Lab Instruments |
| X Dietetics | X DRG Grouper | X Consult/ Request Tracking | X Automated Med Info Exchange |
| X Fee Basis | X DSS Extracts | X Controlled Substances | X Capacity Management - RUM |
| X GRECC | X Education Tracking | X Credentials Tracking | X Capacity Management Tools |
| X HINQ | X Engineering | X Discharge Summary | X Clinical Info Resource Network |
| X IFCAP | X Event Capture | X Drug Accountability | X Clinical Monitoring System |
| X Imaging | X Extensible Editor | X EEO Complaint Tracking | X Enrollment Application System |
| X Kernal | X Health Summary | X Electronic Signature | X Equipment/ Turn-in Request |
| X Kids | X Incident Reporting | X Event Driven Reporting | X Gen. Med.Rec. - Generator |
| X Lab Service | X Intake/ Output | X External Peer Review | X Health Data and Informatics |
| X Letterman | X Integrated Billing | X Functional Independence | X ICR - Immunology Case Registry |
| X Library | X Lexicon Utility | X Gen. Med. Rec. - I/O | X Income Verification Match |
| X Mailman | X List Manager | X Gen. Med. Rec. - Vitals | X Incomplete Records Tracking |
| X Medicine | X Mental Health | X Generic Code Sheet | X Interim Mangement Support |
| X MICOM | X MyHealthEVet | X Health Level Seven | X Master Patient Index VistA |
| X NDBI | X National Drug File | X Hospital Based Home Care | X Missing Patient Reg (Original) A4EL |
| X NOIS | X Nursing Service | X Inpatient Medications | X Order Entry/ Results Reporting |
| X Oncology | X Occurrence Screen | X Integrated Patient Funds | X PCE Patient Care Encounter |
| X PAID | X Patch Module | X MCCR National Database | X Pharmacy Benefits Mangement |
| X Prosthetics | X Patient Feedback | X Minimal Patient Dataset | X Pharmacy Data Management |
| X QUASER | X Police & Security | X National Laboratory Test | X Pharmacy National Database |
| X RPC Broker | X Problem List | X Network Health Exchange | X Pharmacy Prescription Practice |
| X SAGG | X Progress Notes | X Outpatient Pharmacy | X Quality Assurance Integration |
| X Scheduling | X Record Tracking | X Patient Data Exchange | X Quality Improvement Checklist |
| X Social Work | X Registration | X Patient Representative | X Radiology/ Nuclear Medicine |
| X Surgery | X Run Time Library | X PCE Patient/ HIS Subset | X Release of Information - DSSI |
| X Toolkit | X Survey Generator | X Security Suite Utility Pack | X Remote Order/ Entry System |
| Unwinder | X Utilization Review | X Shift Change Handoff Tool | X Utility Management Rollup |
| X VA Fileman | X Visit Tracking | X Spinal Cord Dysfunction | X CA Verified Components - DSSI |
| X VBECS | X VistALink Security | X Text Integration Utilities | X Vendor - Document Storage Sys |
| X VDEF | X Women's Health | X VHS & RA Tracking System | X Visual Impairment Service Team ANRV |
| X VistALink | | X Voluntary Timekeeping | X Voluntary Timekeeping National |

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 minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: Minor Applications

Which of these are sub-components of your system?

1184 Web	ENDSOFT	RAFT
A4P	Enterprise Terminology Server & VHA Enterprise Terminology Services	RALS
		X

(FY 2011) PIA: Final Signatures

Facility Name: REGION 4 > VHA > VISN 01 > Manchester VAMC > LAN

Title:	Name:	Phone:	Email:
--------	-------	--------	--------

Privacy Officer:	Shirley S. Martin	(603) 624-4366, ext. 6700	shirley.martin2@va.gov
------------------	-------------------	------------------------------	------------------------

Information Security Officer:	Mary R. Ballard	(603) 626-6537	mary.ballard@va.gov
-------------------------------	-----------------	----------------	---------------------

System Owner/ Chief Information Officer:	John A. Foote	(603) 624-4366, ext. 6618	john.foote@va.gov
--	---------------	------------------------------	-------------------

Information Owner:	for John J. Galvin	(518) 626-6244	jack.galvin@va.gov
--------------------	--------------------	----------------	--------------------

Other Titles:	0	0	0
---------------	---	---	---

Date of Report:	1/0/00
OMB Unique Project Identifier	029-00-02-00-01-1120-00
Project Name	REGION 4 > VHA > VISN 01 > Manchester VAMC > LAN