

(FY 2010) PIA: System Identification

Program or System Name: LAN Butler Veterans Affairs Medical Center

OMB Unique System /

Application / Program Identifier

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

Description of System /
Application / Program:

The Butler Veterans Affairs Medical Center uses the Local Area Network (LAN) as a General Support System, supporting mission-critical and other systems necessary to conduct day-to-day operations within the Veterans Health Administration. Applications and devices within the LAN support numerous areas, including medical imaging, supply management, decision support, medical research, and education. The Local Area Network is physically located on a government-owned facility and housed within government-owned buildings in Butler, PA. All essential LAN equipment to include routers, switches, and servers are located in locked rooms. The LAN is comprised of two Cisco 6513 routers and 40 Cisco 3750 switches located in 25 closets throughout the Medical Center. The two Cisco 6513 routers are located in building 1. The DS3 circuit, which is provided by Sprint, terminates in building 1. All LAN equipment is equipped with a UPS or emergency power supply.

Facility Name: Butler Veterans Affairs Medical Center

Title:	Name:	Phone:	Email:
Privacy Officer:	Laura Jordan	724-282-5611	Laura.Jordan@va.gov
Information Security Officer:	Kirk Hastings	724-285-2409	Kirk.Hastings@va.gov
Chief Information Officer:	Jupe Fowkes	724-285-5517	Jupe.Fowkes@va.gov
Person Completing Document:	Kirk Hastings	724-285-2409	Kirk.Hastings@va.gov
Other Titles: Chief Technical Officer	Glenn Shaffer	724-285-2405	Glenn.Shaffer@va.gov

Other Titles:
Other Titles:
Date of Last PIA Approved by
VACO Privacy Services:
(MM/YYYY) 08/2009
Date Approval To Operate
Expires: 08/2011

What specific legal authorities
authorize this program or
system: Title 38, United States Code, section 7301(a).

What is the expected number
of individuals that will have
their PII stored in this system: The Butler VAMC LAN provides access and authentication to allow a user to interface with Butler VistA system resources. Butler VistA stores the personal information of approximately 73,000 individuals. It also supports the business functions and provides network storage for over 650 employees working at the Butler VAMC.

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. 04/1998

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): 10/2009

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

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

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

(FY 2010) PIA: System of Records

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

Yes

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

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

1. All System of Record Identifier(s) (number):

79VA19

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://vawww.vhaco.va.gov/privacy/SystemofRecords.htm>

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

Yes

Does the System of Records Notice require modification or updating?

No

(Please Select Yes/No)

Is PII collected by paper methods?

Yes

Is PII collected by verbal methods?

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)	VA File Database	Privacy protected on a secured file server	Automated	Automated
Family Relation (spouse, children, parents, grandparents, etc)	VA File Database	Privacy protected on a secured file server	Written	Automated
Service Information	VA File Database	Privacy protected on a secured file server	Automated	Automated
Medical Information	VA File Database	Privacy protected on a secured file server	Automated	Automated
Criminal Record Information	VA File Database	Privacy protected on a secured file server	Automated	Automated
Guardian Information	VA File Database	Privacy protected on a secured file server	Automated	Automated
Education Information	VA File Database	Privacy protected on a secured file server	Automated	Automated
Benefit Information	VA File Database	Privacy protected on a secured file server	Automated	Automated
Other (Explain)	VA File Database	Privacy protected on a secured file server	Automated	Automated

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Criminal Record Information	Yes	VA Files / Databases (Identify file)	Mandatory	

Guardian Information	Yes	VA Files / Databases (Identify file)	Mandatory
Education Information	Yes	VA Files / Databases (Identify file)	Mandatory
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory
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	purpose of ensuring benefits are received	Both PII & PHI	Privacy Act
Other Veteran Organization	VSO	Yes	to assist veterans with their benefits	Both PII & PHI	Privacy Act
Other Federal Government Agency	CDC	Yes	to protect the public communities	Both PII & PHI	Privacy Act
State Government Agency	Department of Health/Department of Transportation/ State Cancer Registry/ State Health and Statistics	Yes	to protect the public communities	Both PII & PHI	Privacy Act
Local Government Agency	Police Departments/Coroner/ American Red Cross/ Area Agency on Aging	Yes	to protect the public communities	Both PII & PHI	Privacy Act
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: DOD

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

If information is gathered from an individual, is the information provided:
 Through a Written Request
 Submitted in Person
 Online via Electronic Form

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

(FY 2010) PIA: Secondary Use

Will PII data be included with any
secondary use request?

No

- Drug/Alcohol Counseling Mental Health HIV
 Research Sickle Cell Other (Please Explain)
-

if yes, please check all that apply:

Describe process for authorizing access
to this data.

Answer:

(FY 2010) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public? No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: Is collected in accordance with MCM IM-19 Privacy Policy and IM-32 Documentation of Patient Care.

How is data checked for completeness?

Answer: Medical Records are reviewed in accordance with MCM IM-21 Medical Record Review.

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

Answer: Medical Records are reviewed in accordance with MCM IM-21 Medical Record Review.

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

Answer: Medical Records are reviewed in accordance with MCM IM-21 Medical Record Review.

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: 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.

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 90). 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.

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 <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Is security testing conducted on at <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Are performance evaluations conducted on at <u>least</u> 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? If 'No' please describe why:	Yes
Answer: In accordance with VA Handbook 6500, Information Security Program, Appendix D.3. VA requires that facilities control all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verify individual access authorizations before granting access to the facilities. The facilities also control access to areas officially designated as publicly accessible, as appropriate, in accordance with the facility's assessment of risk. The facility controls physical access to the information system independent of the physical access controls for the facility.	
Explain how the project meets IT security requirements and procedures required by federal law. Answer: At the Department level the National Security Operations Center (NSOC) 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 VistA-Legacy is and has been subject to. In addition, (NSOC) 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.	

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 checked="" type="checkbox"/> Bomb Threats | <input checked="" type="checkbox"/> Power Loss |
| <input checked="" type="checkbox"/> Cold/Frost/Snow | <input type="checkbox"/> Sabotage/Terrorism |
| <input checked="" type="checkbox"/> Communications Loss | <input 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 checked="" type="checkbox"/> Denial of Service Attacks | <input type="checkbox"/> Errors (Configuration and Data Entry) |
| <input type="checkbox"/> Earthquakes | <input 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"/> Continuity 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: Privacy and 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 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	X	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)	X	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)	X	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)	X	RAI/MDS
Web Automated Folder Processing System (WAFPS)		Inforce	X	ASSISTS
Courseware Delivery System (CDS)		Awards	X	MUSE
Electronic Performance Support System (EPSS)		Actuarial		Bbraun (CP Hemo)
Veterans Service Representative (VSR) Advisor		Insurance Self Service	X	VIC
Loan Guaranty Training Website		Insurance Unclaimed Liabilities	X	BCMA Contingency Machines
C&P Training Website		Insurance Online	X	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	X	BIRLS
Telecare Record Manager		Centralized Accounts Receivable System (CARS)
Omnicell	X	Compensation & Pension (C&P)
Powerscribe Dictation System		Corporate Database
EndoSoft		Control of Veterans Records (COVERS)
Compensation and Pension (C&P)	X	Data Warehouse
Montgomery GI Bill	X	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	X	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)*

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

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
		<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?		

OUTPATIENT PHARMACY	SOCIAL WORK
PAID	SPINAL CORD DYSFUNCTION
PATCH MODULE	SURGERY
PATIENT DATA EXCHANGE	SURVEY GENERATOR
PATIENT FEEDBACK	TEXT INTEGRATION UTILITIES
PATIENT REPRESENTATIVE	TOOLKIT
PCE PATIENT CARE	UNWINDER
ENCOUNTER	UTILIZATION MANAGEMENT ROLLUP
PCE PATIENT/IHS SUBSET	
PHARMACY BENEFITS	UTILIZATION REVIEW
MANAGEMENT	
PHARMACY DATA	VA CERTIFIED COMPONENTS - DSSI
MANAGEMENT	
PHARMACY NATIONAL	VA FILEMAN
DATABASE	
PHARMACY PRESCRIPTION	VBECs
PRACTICE	
POLICE & SECURITY	VDEF
PROBLEM LIST	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES	VHS&RA ADP TRACKING SYSTEM
PROSTHETICS	VISIT TRACKING
QUALITY ASSURANCE	VISTALINK
INTEGRATION	
QUALITY IMPROVEMENT	VISTALINK SECURITY
CHECKLIST	
QUASAR	VISUAL IMPAIRMENT SERVICE TEAM
	ANRV
RADIOLOGY/NUCLEAR	VOLUNTARY TIMEKEEPING
MEDICINE	
RECORD TRACKING	VOLUNTARY TIMEKEEPING NATIONAL
REGISTRATION	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: Butler Veterans Affairs Medical Center

Title:	Name:	Phone:	Email:
Privacy Officer:	Laura Jordan	724-282-5611	Laura.Jordan@va.gov
Digital Signature Block			
Information Security Officer:	Kirk Hastings	724-285-2409	Kirk.Hastings@va.gov
Digital Signature Block			
Chief Information Officer:	Jupe Fowkes	724-285-5517	Jupe.Fowkes@va.gov
Digital Signature Block			
Person Completing Document:	Kirk Hastings	724-285-2409	Kirk.Hastings@va.gov
Digital Signature Block			
System / Application / Program Manager:	Glenn Shaffer	724-285-2405	Glenn.Shaffer@va.gov
Digital Signature Block			

Date of Report: 10/1/2009
 OMB Unique Project Identifier: 029-00-02-00-01-1120-00
 Project Name: LAN Butler Veterans Affairs Medical Center