

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

### **Roles and Responsibilities:**

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the 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, 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**

**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](mailto:christina.pettit@va.gov) to received full credit for submission.

(FY 2011) PIA: System Identification

Program or System Name:

REGION 1 VHA VISN 22 San Diego VAMC LAN

OMB Unique System / Application / Program Identifier  
(AKA: UPIID #):029-00-02-00-01-1120-00

Description of System/ Application/ Program:  
The Local Area Network (LAN) provides internal and external network connectivity for users to access major VA applications at the VASDHS. Applications include VISTA/CPRS, Windows 2003 Active Directory, Microsoft Exchange application and database servers, PACs, and the PBX systems.

Facility Name:

VA San Diego Healthcare System (VASDHS)

Title:	Name:	Phone:	Email:
Privacy Officer:	Mike Deshazer	858.642.3491	mike.deshazer@va.gov
Information Security Officer:	Jesse Christmas	858.642.6200	jesse.christmas@va.gov
System Owner/ Chief Information Officer:	Duc Nguyen	858.642-3399	duc.d.nguyen@va.gov
Information Owner:	Duc Nguyen	858.642-3399	duc.d.nguyen@va.gov
Other Titles: ISO	Kathleen DeVerno	858.642.1021	kathleen.devverno@va.gov
Other Titles: ISO	Jeanne Pham	858.642.1559	dua.pham2@va.gov
Person Completing Document:	Jesse Christmas	858.642.6200	jesse.christmas@va.gov

Other Titles:  
Date of Last PIA Approved by VACO Privacy: 08/2008  
Date Approval To Operate Expires: 08/2011  
What Specific Legal Authorities Authorize This

program or system: 38 USC 7301  
What is the expected number of individuals that will Identify what stage the System / Application / 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.

01/1997  
Is there an authorized change control process which documents any changes to existing applications or systems? Yes

If No, please explain: Yes

Has a PIA been completed within the last three years? Yes

Date of Report (MM/YYYY): 12/2010

2. System Identification

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

**(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): 24VA19  
Patient Medical Records-VA
2. Name of the System of Records: http://www.privacy.va.gov/privacy\_impact\_assessment.asp
3. Location where the specific applicable System of Records Notice may be accessed (include the URL): t.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? No
- 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? No
- Authority: Does the privacy notice specify the effects of providing information on a voluntary basis? No
- Disclosures: Does the privacy notice specify routine use(s) that may be made of the information? No

(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	Information collected for patient care	All	All
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Information collected for patient care	All	All
Service Information	ALL	Information collected for patient care	All	All
Medical Information	ALL	Information collected for patient care	All	All
Criminal Record Information				
Guardian Information	ALL	Information collected for patient care	All	All
Education Information	ALL	Information collected for patient care	All	All
Benefit Information	ALL	Information collected for benefits and payment	All	All
Other (Explain)	N/A			

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	Both mandatory and Voluntary
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Voluntary	Both mandatory and Voluntary

Service Information	Yes	VA Files / Databases (Identify file)	Mandatory	Both mandatory and Voluntary
Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory	Both mandatory and Voluntary
Criminal Record Information	No			Both mandatory and Voluntary
Guardian Information	Yes	VA Files / Databases (Identify file)	Mandatory	Both mandatory and Voluntary
Education Information	Yes	VA Files / Databases (Identify file)	Mandatory	Both mandatory and Voluntary
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	Both mandatory and Voluntary
Other (Explain)				
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	VASDHS	Yes	VASI used in daily ops	Both PII & PHI	VA Directive 6500
-----------------------------------	--------	-----	------------------------	----------------	-------------------

Other Veteran Organization					
----------------------------	--	--	--	--	--

Other Federal Government Agency	DOD	Yes	VASI used in daily ops	Both PII & PHI	VA Directive 6500
---------------------------------	-----	-----	------------------------	----------------	-------------------

State Government Agency		No			
-------------------------	--	----	--	--	--

Local Government Agency		No			
-------------------------	--	----	--	--	--

Research Entity		No			
-----------------	--	----	--	--	--

Other Project / System					
------------------------	--	--	--	--	--

Other Project / System					
------------------------	--	--	--	--	--

Other Project / System					
------------------------	--	--	--	--	--

(FY 2011) PIA: Access to Records

Does the system gather information from another system? VISTA RO Yes

Please enter the name of the system: VISTA RO

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 2011) PIA: Secondary Use

Will PII data be included with any secondary use request? No

if yes, please check all that apply:

Drug/Alcohol Counseling  Mental Health  HIV

Research  Sickle Cell  Other (Please Explain)

Describe process for authorizing access to this data.

## (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: Minimum use policy enforcement

How is data checked for completeness?

Answer: User or information owner

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

Answer: Information owner is responsible

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

Answer: Information Owner and User of the date are responsible

*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: Information is retained according to the VA Records Control Schedule (RCS-10) for future treatment of the patients, for research purposes, and legal issues. and to investigate cause/effect of agents that were used during combat, i.e, Agent Orange to determine to the long term effect on the veteran population. 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 (RCS-10) 10-1, Item XIII, 2.b. (Page 190). Researchers are responsible for destroying research records as per the RCS which is undergoing revision.

Paper records shipped to the national archive will be destroyed by the agency after the 75 year retention requirement is met.

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

Answer: The retention is set by the Record Control Schedule (RCS-10) and varies according the documents. Information needs to be retained to document VA business for future reference.

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

Answer: Information is retained according to the VA Records Control Schedule (RCS-10) for future treatment of the patients, for research purposes, and legal issues, and to investigate cause/effect of agents that were used during combat, i.e, Agent Orange to determine to the long term effect on the veteran population. 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 (RCS-10) 10-1, Item XLIII, 2.b. (Page 190). Researchers are responsible for destroying research records as per the RCS which is undergoing revision.  
Paper records shipped to the national archive will be destroyed by the agency after the 75 year retention requirement is met.

Where are these procedures documented?

Answer: VA Directive 6300.1, Record Management Procedures, Record Control Schedule (RCS-10), VA Directive 6371 and current VA standards on the disposal of sensitive information

How are data retention procedures enforced?

Answer: Field records officers are responsible for records management activities at this facility. In addition, ITOC will review record management procedures when they conduct audits.

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.

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: VASDHS is configured according to R1 guidelines.

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

Answer: (Other Risks)

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: Security Controls to mitigate misuse of information

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.

### 7. Security

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; 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:*

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: Additional 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	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 Performance 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)
Bhraun (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	Educational 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)
Endsoft	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 Entitlement Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Assistant	Service Member Records Tracking System
Omnicell	National Silent Monitoring (NSM)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Powerscribe Dictation System	Systematic Technical Accuracy Review (STAR)
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
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)

### 9. VBA Minor Applications

VBA Data Warehouse	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?

Which of these are sub-components of your system?

(FY 2011) PIA: VISTA Minor Applications

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

(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
Administrative Data Repository (ADR)	ePROMISE	Remedy Application
ADT	EYECAP	X SAN
Agent Cashier	Financial and Accounting System (FAS)	Scanning Exam and Evaluation System
X Air Fortress	Financial Management System	Sentillion
Auto Instrument	Genesys	Stellant
Automated Access Request	Health Summary Contingency	Stentor
BDN 301	ICB	X Tracking Continuing Education
Bed Board Management System	KOWA	X Traumatic Brain Injury
Cardiff Teleform	Lynx Duress Alarm	X VA Conference Room Registration
Cardiology Systems (stand alone servers from the network)	MHTP	VAMedSafe
X CHECKPOINT	Microsoft Active Directory	VBA Data Warehouse
Clinical Data Repository/Health Data Repository	Microsoft Exchange E-mail System	VHAHUNAPP1
Combat Veteran Outreach Committee on Waiver and Compromises	Military/Vet Eye Injury Registry	VHAHUNFPc1
CP&E	Mumps AudioFAX	VISTA RAD
Crystal Reports Enterprise	NOAHLINK	Whiteboard
X Data Innovations	Omnicell	
DELIVEREX	Onvicord (VLOG)	
	Optifill	

11. Minor Applications

DICTATION-Power Scribe	
DRM Plus	X
DSIT	
DSS Quadramed	
EDS-Whiteboard (AVJED)	
EKG System	X
Embedded Fragment Registry	
P2000 ROBOT	
PACS database	
Personal Computer Generated Letters	
PICIS OR	
PIV Systems	
Q-Matic	
QMSI Prescription Processing	

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name comments you may wish to include.

Name	Human Resources BI Tracker
Description	Access DB for background investigations.
Comments	Limited to HR ISOs, and Research POC
Is PII collected by this minor application? Yes	
Does this minor application store PII? Yes	
If yes, where?	Access DB for background investigations.
Who has access to this data	Limited to HR, ISOs

Name	TBI Polytrauma Tracking System
Description	Tool for tracking TBI patients visits at facility clinics.
Comments	
Is PII collected by this minor application? Yes	
Does this minor application store PII? Yes	
If yes, where?	Network Server
Who has access to this data?	Limited to TBI Staff

Name	Patient Event Report System (PERS)
Description	Tool for tracking pateint events
Comments	
Is PII collected by this minor application? Yes	
Does this minor application store PII? Yes	
If yes, where?	Network Server

11. Minor Applications

Who has access to this data?

PIMS and limited clinical Staff

11. Minor Applications

(FY 2011) PIA: Final Signatures

Facility Name: REGION 1 VHA VISN 22 San Diego VAMC LAN

Title: Name: Phone: Email:

Privacy Officer: Mike Deshazer 858.642.3491 mike.deshazer@va.gov

Information Security Officer: Jesse Christmas 858.642.6200 jesse.christmas@va.gov  


System Owner/Chief Information Officer: Duc Nguyen 858.642-3399 duc.d.nguyen@va.gov  


Information Owner: Duc Nguyen 858.642-3399 duc.d.nguyen@va.gov  


Other Titles: Associate Chief Ruey Keller 858.642.6420 ruey.keller@va.gov  


Date of Report: 1/21/2011  
OMB Unique Project Identifier: 029-00-02-00-01-1120-00

Project Name: REGION 1 VHA VISN 22 San Diego VAMC LAN