Welcome to the PIA for FY 2010!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program. More information can be found by reading VA 6508.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vaww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

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

a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Handbook 6202.2.

b. Records Officer is responsible for supplying records retention and deletion schedules.

c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Handbook 6202.2 and to immediately report all anomalies to the Privacy Service and appropriate management chain.

d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.

e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and 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 indentify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at

(FY 2010) PIA: System Identification

Program or System Name:	Region 5 > VBA > San Diego Region > VARO Ft Harrison > LAN
OMB Unique System / Application / Program Identifier (AKA: UPID #):	029-00-02-00-01-1120-00
Description of System / Application / Program:	The Regional Office (RO) Local Area Network (LAN) serves as the default repository for incidental data used and processed by various VBA Major Applications. This data is used in granting compensation, pension, education, vocational rehabilitation and employment, insurance, and loan guaranty benefits to veterans. Information stored also includes data used for various administrative functions. The system provides RO employees local access to file and print sharing services on the LAN. It also provides client access to various applications, including email.
Facility Name:	Ft Harrison RO

Title:	Name:	Phone:
Privacy Officer:	Donna Church	406-495-2031
Information Security Officer:	Kristy Ritter	801-326-1782
Chief Information Officer:	Arthur Fusco	619-400-5692
Person Completing Document:	Donna Church and Kristy Ritter	406-495-2031
Other Titles: System Owner	Kevin C. Causley	202-461-9170
Other Titles:		
Other Titles:		

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	08/2008
Date Approval To Operate Expires:	08/2011

What specific legal authorities authorize this program or system:	Title 38 of the United States Code
What is the expected number of individuals that will have their PII stored in this system:	1,000,000 - 99,999,999
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.	20 Years
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes
If No, please explain:	
Has a PIA been completed within the last three years?	Yes

Date of Report (MM/YYYY):

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

Email:
donna.church@va.gov kristy.ritter@va.gov arthur.fusco@va.gov donna.church@va.gov

n.

rforming work for the VA?

ool, or other PII data?

n of PII)

(FY 2010) PIA: System of Records

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

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):

2. Name of the System of Records:
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):

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

Does the System of Records Notice require modification or updating?

Is PII collected by paper methods?
Is PII collected by verbal methods?
Is PII collected by automated methods?
Is a Privacy notice provided?

Proximity and Timing: Is the privacy notice provided at the time of data collection?
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

Yes

55VA26, 58VA21/22/28, 38VA21, 36VA00, 46VA00, 53VA00

Loan Guaranty Home, Loan Guaranty Home, Condominium and Manufactured Home Loan Applicant Records, Specially Adapted Housing Applicant Records, and Vendee Loan Applicant Records--VA, Compensation, Pension, Education and Rehabilitation Records-VA, Veterans and Beneficiaries Identification Records Location Subsystem--VA. 36VA00 Veterans and Armed Forces Personnel United States Government Life Insurance Records-VA. 46VA00 Veterans, Beneficiaries and Attorneys United States Government Insurance Award Records-VA. 53VA00 Veterans Mortgage Life Insurance-VA, Veterans and Beneficiaries Identification and Records Locations (BIRLS) and Compensation, Pension, Education, and Rehabilitation (covers BDN and Corporate databases)

http://www.rms.oit.va.gov/System_of_Records.asp

Yes

No

(Please Select Yes/No)

Yes

Yes

Yes

Yes

Yes

Yes

Yes

Yes

(FY 2010) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	ALL	Benefits	All	All
Family Relation (spouse, children, parents, grandparents, etc)	Paper	Benefits	Written	Written
Service Information	Paper	Benefits	Written	Written
Medical Information	Paper	Benefits	Written	Written
Criminal Record Information	Paper	Benefits	Verbal & Written	Verbal & Written
Guardian Information	Paper	Benefits	Written	Written
Education Information	Paper	Benefits	Written	Written
Benefit Information	Paper	Benefits	Verbal & Written	Verbal & Written
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Voluntary	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	
Service Information	Yes	Veteran	Voluntary	
Medical Information	Yes	Veteran	Voluntary	
Criminal Record Information	Yes	Veteran	Voluntary	
Guardian Information	Yes	Veteran	Voluntary	
Education Information	Yes	Veteran	Voluntary	
Benefit Information	Yes	Veteran	Voluntary	
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	VHA/VBA	Yes	Benefits	Both PII & PHI	VA Directive 6500, M20-4, Part II, VBA IRM Handbook 5.00.02HB2 and M20-4, Part II, VBA IRM Handbook 5.00.02HB4, 38 CFR 1.550 through 1.559, VA Handbook 6300, VA Handbook 6300.1, VA Handbook 6300.3
Other Veteran Organization	Veterans Service Organizations	Yes	Read only access BDN, Covers, Share, Virtual VA	Both PII & PHI	VA Directive 6500, M20-4, Part II, VBA IRM Handbook 5.00.02HB2 and M20-4, Part II, VBA IRM Handbook 5.00.02HB4, 38 CFR 1.550 through 1.559, VA Handbook 6300, VA Handbook 6300.1, VA Handbook 6300.3

Other Federal Government Agency	National Serivce Life Insurance, Veterans Mortgage Life Insurance, Veterans Government Life Insurance verifies if a veteran is deceased. The Social Security Administration also verifies if a veteran is deceased and provides income verification, SSN match. Department of Defense provides (1) Service Data; reserve and guard participation, retired pay or severance pay, hazardous agent exposure, branch of service, active duty date, released date, type of discharge, separation reason; and (2) Medical Records: Military clinical records, government health records, vocational rehabilitation and employment records, line of duty investigations. Other Federal agencies that	Yes	Verifies if veteran is deceased	Both PII & PHI	VA Directive 6500, M20-4, Part II, VBA IRM Handbook 5.00.02HB2 and M20-4, Part II, VBA IRM Handbook 5.00.02HB4, 38 CFR 1.550 through 1.559, VA Handbook 6300, VA Handbook 6300.1, VA Handbook 6300.3
State Government Agency	Montana Department of Veteran Services	Yes	Read only access BDN, Covers, Share, Virtual VA	PII	VA Directive 6500, M20-4, Part II, VBA IRM Handbook 5.00.02HB2 and M20-4, Part II, VBA IRM Handbook 5.00.02HB4, 38 CFR 1.550 through 1.559, VA Handbook 6300, VA Handbook 6300.1, VA Handbook 6300.3
Local Government Agency					
Research Entity					
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2010) PIA: Access to Records

Does the system gather information from another system?	No
Please enter the name of the system:	
Per responses in Tab 4, does the system gather information from an individual?	Yes
If information is gathered from an individual, is the information provided:	☑ Through a Written Request ☑ Submitted in Person ☑ Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	No

(FY 2010) 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. 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: Information is collected primarily on defined forms and entered to specific fields of database records. The required veteran's data is stored within the databases, which support the individual benefits the veteran applied and or has been granted. The LAN accesses these databases to retrieve the data.

How is data checked for completeness?

Answer: Data is checked for completeness by system audits, manual verifications and annual questionnaires through automated veteran letters. These letters ask specific questions for verification based on the existing entitlement or benefit the veteran is receiving. Match programs notify and we ensure that collected data is accurate. Also, data are updated with each veteran correspondence.

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

Answer: Data are updated as a result of returned mail, or returned direct deposits, or through contract with the veteran, beneficiary, or power of attorney. Additionally, verifications and system audits are performed.

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

Answer: All data are matched against supporting claims documentation submitted by the veteran, widow or dependent. Certain data such as SSN is verified with the Social Security Administration. Prior to any award or entitlement authorization(s) by the VBA, the veteran record is manually reviewed and data validated to ensure correct entitlement has been approved.

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: Date retention policies and procedures are being updated. The update will evaluate existing data retention practices against current best practices and department and Federal Government guidance.

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

Answer: Data is stored in accordance with the Records Control Schedule

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

Answer: Following the end of the retention schedule in accordance with the Records Control Schedule, data is maintained and destroyed.

Where are these procedures documented?
Answer: Records Control Schedule and other pertinent regulatory guidance.

How are data retention procedures enforced?
Answer: Following end of FY - Records Manager conducts review of admin type files. Recommend development system to ensure appropriate tracking/retion of files not maintained in the common admin area.

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

Yes

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2010) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13? No

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 2010) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	Yes
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..	Yes
Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes

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

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

If 'No' please describe why:
Answer:

Explain how the project meets IT security requirements and procedures required by federal law.
Answer: An annual assessment of security controls is currently conducted and will continue to be conducted to ensure that IT security requirements are being met. This strategy implements Federal Regulations, VA IT security policy and guidelines and NIST Guidelines. Security is implemented in compliance with VA's guidelines, policies, and mandates.

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

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

Answer: (Other Risks)

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

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

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: As a result of performing the PIA, continual emphasis and attention will be applied to addressing security and privacy concerns including assuring that collection of data and personal information contains appropriate consent and release information and that all information stored on VBA/Region Five LANs are secured per VA security standards.

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)

- [x] 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)

- [x] 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)

- [x] The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- [ ] The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
- [ ] The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments?
The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:

(FY 2010) PIA: Additional Comments

Add any additional comments on this tab for any question in the form you want to comment on.
Please indicate the question you are responding to and then add your comments.

(FY 2010) PIA: VBA Minor Applications

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

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

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

	Name	Description	Comments
Minor app #1			

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

	Name	Description	Comments
Minor app #2			

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

	Name	Description	Comments
Minor app #3			

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

Baker System		Veterans Assistance Discharge System (VADS)
Dental Records Manager		VBA Training Academy
Sidexis	x	Veterans Service Network (VETSNET)
Priv Plus		Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
Mental Health Asisstant	x	BIRLS
Telecare Record Manager		Centralized Accounts Receivable System (CARS)
Omnicell	x	Compensation & Pension (C&P)
Powerscribe Dictation System	x	Corporate Database
EndoSoft	x	Control of Veterans Records (COVERS)
Compensation and Pension (C&P)		Data Warehouse
Montgomery GI Bill		INS - BIRLS
Vocational Rehabilitation & Employment (VR&E) CH 31		Mobilization
Post Vietnam Era educational Program (VEAP) CH 32	x	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 Entitelment 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
ADP PLANNING (PLANMAN)
ADVERSE REACTION TRACKING
ASISTS
AUTHORIZATION/SUBSCRIPTION
AUTO REPLENISHMENT/WARD STOCK
AUTOMATED INFO COLLECTION SYS
AUTOMATED LAB INSTRUMENTS
AUTOMATED MED INFO EXCHANGE
BAR CODE MED ADMIN
BED CONTROL
BENEFICIARY TRAVEL
CAPACITY MANAGEMENT - RUM
CAPRI
CAPACITY MANAGEMENT TOOLS
CARE MANAGEMENT
CLINICAL CASE REGISTRIES
CLINICAL INFO RESOURCE NETWORK
CLINICAL MONITORING SYSTEM
CLINICAL PROCEDURES
CLINICAL REMINDERS
CMOP
CONSULT/REQUEST TRACKING
CONTROLLED SUBSTANCES
CPT/HCPCS CODES
CREDENTIALS TRACKING
DENTAL
DIETETICS
DISCHARGE SUMMARY
DRG GROUPER
DRUG ACCOUNTABILITY
DSS EXTRACTS
EDUCATION TRACKING
EEO COMPLAINT TRACKING
ELECTRONIC SIGNATURE
ENGINEERING
ENROLLMENT APPLICATION SYSTEM
EQUIPMENT/TURN-IN REQUEST
EVENT CAPTURE
EVENT DRIVEN REPORTING
EXTENSIBLE EDITOR
EXTERNAL PEER REVIEW
FEE BASIS
FUNCTIONAL INDEPENDENCE
GEN. MED. REC. - GENERATOR
GEN. MED. REC. - I/O
GEN. MED. REC. - VITALS
GENERIC CODE SHEET
GRECC
HEALTH DATA & INFORMATICS
HEALTH LEVEL SEVEN
HEALTH SUMMARY
HINQ
HOSPITAL BASED HOME CARE
ICR - IMMUNOLOGY CASE REGISTRY
IFCAP
IMAGING
INCIDENT REPORTING
INCOME VERIFICATION MATCH
INCOMPLETE RECORDS TRACKING
INPATIENT MEDICATIONS
INTAKE/OUTPUT
INTEGRATED BILLING
INTEGRATED PATIENT FUNDS
INTERIM MANAGEMENT SUPPORT
KERNEL
KIDS
LAB SERVICE
LETTERMAN
LEXICON UTILITY
LIBRARY
LIST MANAGER
MAILMAN
MASTER PATIENT INDEX VISTA
MCCR NATIONAL DATABASE
MEDICINE
MENTAL HEALTH
MICOM
MINIMAL PATIENT DATASET
MYHEALTHEVET
Missing Patient Reg (Original) A4EL
NATIONAL DRUG FILE
NATIONAL LABORATORY TEST
NDBI
NETWORK HEALTH EXCHANGE
NOIS
NURSING SERVICE
OCCURRENCE SCREEN
ONCOLOGY
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.

	Name		Description		Comments
			Is PII collected by this min or application?		
Minor app #1			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?		
Minor app #2			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?		
Minor app #3			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

OUTPATIENT PHARMACY

PAID
PATCH MODULE
PATIENT DATA EXCHANGE

PATIENT FEEDBACK

PATIENT REPRESENTATIVE

PCE PATIENT CARE ENCOUNTER
PCE PATIENT/IHS SUBSET

PHARMACY BENEFITS MANAGEMENT
PHARMACY DATA MANAGEMENT
PHARMACY NATIONAL DATABASE

PHARMACY PRESCRIPTION PRACTICE
POLICE & SECURITY

PROBLEM LIST

PROGRESS NOTES

PROSTHETICS
QUALITY ASSURANCE INTEGRATION
QUALITY IMPROVEMENT CHECKLIST
QUASAR

RADIOLOGY/NUCLEAR MEDICINE
RECORD TRACKING

REGISTRATION

RELEASE OF INFORMATION - DSSI

REMOTE ORDER/ENTRY SYSTEM
RPC BROKER

RUN TIME LIBRARY
SAGG
SCHEDULING

SECURITY SUITE UTILITY PACK

SHIFT CHANGE HANDOFF TOOL

SOCIAL WORK

SPINAL CORD DYSFUNCTION
SURGERY
SURVEY GENERATOR

TEXT INTEGRATION UTILITIES

TOOLKIT

UNWINDER

UTILIZATION MANAGEMENT ROLLUP

UTILIZATION REVIEW

VA CERTIFIED COMPONENTS - DSSI

VA FILEMAN

VBECS

VDEF

VENDOR - DOCUMENT STORAGE SYS

VHS&RA ADP TRACKING SYSTEM

VISIT TRACKING
VISTALINK

VISTALINK SECURITY

VISUAL IMPAIRMENT SERVICE TEAM ANRV
VOLUNTARY TIMEKEEPING

VOLUNTARY TIMEKEEPING NATIONAL

WOMEN'S HEALTH

CARE TRACKER

(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.

	Name		Description		Comments

Minor app #1

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

	Name		Description		Comments

Minor app #2

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

	Name		Description		Comments

Minor app #3

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

(FY 2010) PIA: Final Signatures

Facility Name: Ft Harrison RO

Title	Name	Phone	Email
Privacy Officer:	Donna Church	406-495-2031	donna.church@va.gov
Donna A Church Digital Signature Block			
Information Security Officer:	Kristy Ritter	801-326-1782	kristy.ritter@va.gov
Kristy Ritter Digital Signature Block			
Chief Information Officer:	Arthur Fusco	619-400-5692	arthur.fusco@va.gov
Arthur Fusco Digital Signature Block			
Person Completing Document:	Donna Church and Kristy Ritter	406-495-2031	donna.church@va.gov
Donna A Church Digital Signature Block	Kristy Ritter		
System / Application / Program Manager:	Kevin C. Causley	202-461-9170	kevin.causley@va.gov
BARLEY, MARY, VBAVACO Digital Signature Block	Digitally signed by BARLEY, MARY, VBAVACO DN: o=Department of Veterans Affairs, ou=Dept. of Veterans Affairs, Internal Staff, ou=www.verisign.com/repository/CPS Incorp. by Ref.,LIAB.LTD(c)96, cn=BARLEY, MARY, VBAVACO, email=mary.barley@va.gov Date: 2010.06.28 11:50:15 -04'00'		

Date of Report:	06/22/2010
OMB Unique Project Identifier	029-00-02-00-01-1120-00
Project Name	Region 5 > VBA > San Diego Region > VARO Ft Harrison > LAN