

## **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](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

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 an individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirectly identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

**Macros Must Be Enabled on This Form**

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

## (FY 2010) PIA: System Identification

Program or System Name: VA Region 1 Sacramento RDC LAN

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

The Region 1 RDC General Support System (GSS) provides Local Area Network (LAN) and Wide Area Network (WAN) support as well as IT resources in support of the VA – Region 1 (RDPC)

Description of System / Application / Program: mission.

Facility Name: Sacramento RDC

Title:	Name:	Phone:	Email:
Privacy Officer:	Garnett Best	202-461-7474	<a href="mailto:garnett.best@va.gov">garnett.best@va.gov</a>
Information Security Officer:	Craig Heitz	612-725-2132	<a href="mailto:craig.heiz@va.gov">craig.heiz@va.gov</a>
	Dr. James Laub Regional Director OI&T Region 1		
Chief Information Officer:		480-325-3131	<a href="mailto:james.laub@va.gov">james.laub@va.gov</a>
Person Completing Document:	Craig Heitz	612-725-2132	<a href="mailto:craig.heiz@va.gov">craig.heiz@va.gov</a>

Other Titles:	Sean Mitts, Region 1 Infrastructure Service Line manager	360-619-5924	<a href="mailto:sean.mitts@va.gov">sean.mitts@va.gov</a>
---------------	--	--------------	--

Other Titles:

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)

None

Date Approval To Operate Expires:

N/A

---

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:

1,000,000

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.

06/2005

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?

N/A: First PIA

---

Date of Report (MM/YYYY):

N/A

**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?

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

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

## (FY 2010) PIA: System of Records

---

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

Yes

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

---

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

- |   |   |
|---|---|
| 1. All System of Record Identifier(s) (number):   | 02VA135; 04VA115; 07VA138; 14VA135; 20VA138; 23VA   |
| 2. Name of the System of Records:   | Applicants for Employment under Title 38, USC-VA; Blood D   |
| 3. Location where the specific applicable System of Records Notice may be accessed (include the URL): | <a href="http://vawww.vhaco.va.gov/privacy/SystemofRecords.htm">http://vawww.vhaco.va.gov/privacy/SystemofRecords.htm</a> |
- 

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?

No

Is PII collected by verbal methods?

No

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)	Verbal	What is required by law	Written	Verbally
Family Relation (spouse, children, parents, grandparents, etc)	VA File Database		Written	Verbally
Service Information	VA File Database		Verbally	Verbally
Medical Information	VA File Database		Verbally	
Criminal Record Information	VA File Database			
Guardian Information	VA File Database			
Education Information	VA File Database		Automated	
Benefit Information	VA File Database			
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

Public (identify specific entity)

Mandatory

Clinical and administrative information will be used in the effort to treat and contact the veteran. The most common data types that are captured and accessed on a regular basis by authorized individuals are first and last name, middle initial, DOB, SSN, and address. This patient information falls into two classes: administrative and clinical. Clinical information is used to diagnose, prescribe treatment and follow clinically the patient through his/her health care encounters. Administrative data is used to identify the veteran (SSN), correspond to/from (name and address), and determine eligibility (patient administrative info + SSA and IRS data).

Family Relation (spouse, children, parents, grandparents, etc)

Service Information

Medical Information

In accordance with local facility policy.

Criminal Record Information

In accordance with local facility policy.

Guardian Information

In accordance with local facility policy.

Education Information

In accordance with local facility policy.

Benefit Information

In accordance with local facility policy.

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?
	Region 4		Complete Access		
	Visn 1 Sites				
	Bedford				
	Manchester				
	Northampton				
	Boston Healthcare System (Brockton, Jamaica Plain, West Roxbury)				
	Togus				
	White-River Junction				
	Providence				
Internal Sharing: VA Organization	Connecticut Healthcare System (West-Haven, Newington)				
	Visn 2 Sites				
	Buffalo				
	Batavia				
	Albany				
	Canandaigua				
	Syracuse				
	Bath				
	Visn 3 Sites			Both PII & PHI	Defined at the Facility
		Yes			
Other Veteran Organization		No			Defined at the Facility
Other Federal Government Agency					Defined at the Facility
State Government Agency					Defined at the Facility
Local Government Agency					Defined at the Facility
Research Entity					Defined at the Facility
Other Project / System					
Other Project / System					
Other Project / System					

**(FY 2010) PIA: Access to Records**

---

Does the system gather information from another system?

Defined at the Facility

Please enter the name of the system:

Defined at the Facility

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

Defined at the Facility

If information is gathered from an individual, is the information provided:

- Through a Written Request
- Submitted in Person
- Online via Electronic Form

Defined at the Facility

---

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

---

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? If Yes, Please Specify:	No	Performed at the Facility.
Explain how collected data are limited to required elements: Answer:		Performed at the Facility. Performed at the Facility.
How is data checked for completeness? Answer:		Performed at the Facility. Performed at the Facility.
What steps or procedures are taken to ensure the data remains current and not out of date? Answer:		Performed at the Facility. Performed at the Facility.
How is new data verified for relevance, authenticity and accuracy? Answer:		Performed at the Facility. Performed at the Facility.
<i>Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)</i>		
Answer:		

**(FY 2010) PIA: Retention & Disposal**

What is the data retention period? Answer:		Performed at the Facility. Performed at the Facility.
Explain why the information is needed for the indicated retention period? Answer:		Performed at the Facility. Performed at the Facility.
What are the procedures for eliminating data at the end of the retention period? Answer:		Performed at the Facility. Performed at the Facility.
Where are these procedures documented? Answer:		Performed at the Facility.
How are data retention procedures enforced? Answer:		Performed at the Facility. Performed at the Facility.
Has the retention schedule been approved by the National Archives and Records Administration (NARA) Answer:	Yes	Performed at the Facility.
<i>Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)</i>		
Answer:		

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

Will information be collected through the internet from children under age 13? If Yes, How will parental or guardian approval be obtained? Answer:	No	
--	----	--

(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.

The security of Region 1 RDC LANs have been reviewed by ITOC and have had their security controls assess by STG which is a 3rd party contracted by VA for the 2009 SCA testing. Validation of NIST 800-53 and VAD 6500 as the federal requirements measure was utalized for all reviews. All findins are monitored and tracked through resolution in SMART.

---

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 checked="" type="checkbox"/> Storms/Hurricanes                     |
| <input checked="" type="checkbox"/> Computer Intrusion                   | <input type="checkbox"/> Substance Abuse                                  |
| <input checked="" type="checkbox"/> Data Destruction                     | <input 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 checked="" type="checkbox"/> Errors (Configuration and Data Entry) |
| <input checked="" type="checkbox"/> Earthquakes                          | <input type="checkbox"/> Burglary/Break In/Robbery                        |
| <input checked="" type="checkbox"/> Eavesdropping/Interception           | <input 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"/> Contingency 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: No changes were made to the system as a result of completing the PIA.

---

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 **N/A**

---

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

N/A	Records Locator System Veterans Assistance Discharge System (VADS)  LGY Processing  Loan Service and Claims LGY Home Loans  Search Participant Profile (SPP)  Control of Veterans Records (COVERS)  SHARE Modern Awards Process Development (MAP-D) Rating Board Automation 2000 (RBA2000)  State of Case/Supplemental (SOC/SSOC)  Awards  Financial and Accounting System (FAS)  Eligibility Verification Report (EVR) Automated Medical Information System (AMIS)290  Web Automated Reference Material System (WARMS)  Automated Standardized Performance Elements Nationwide (ASPEN)  Inquiry Routing Information System (IRIS)  National Silent Monitoring (NSM)  Web Service Medical Records (WebSMR)  Systematic Technical Accuracy Review (STAR)  Fiduciary STAR Case Review Veterans Exam Request Info System (VERIS) Web Automated Folder Processing System (WAFPS)  Courseware Delivery System (CDS) Electronic Performance Support System (EPSS) Veterans Service Representative (VSR) Advisor  Loan Guaranty Training Website  C&P Training Website	Education Training Website  VR&E Training Website VA Reserve Educational Assistance Program Web Automated Verification of Enrollment Right Now Web VA Online Certification of Enrollment (VA-ONCE) Automated Folder Processing System (AFPS) Personal Computer Generated Letters (PCGL) Personnel Information Exchange System (PIES) Rating Board Automation 2000 (RBA2000)  SHARE  State Benefits Reference System Training and Performance Support System (TPSS) Veterans Appeals Control and Locator System (VACOLS) Veterans On-Line Applications (VONAPP)  Automated Medical Information Exchange II (AIME II)  Committee on Waivers and Compromises (COWC)  Common Security User Manager (CSUM)  Compensation and Pension (C&P) Record Interchange (CAPRI) Control of Veterans Records (COVERS) Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)  Fiduciary Beneficiary System (FBS) Hearing Officer Letters and Reports System (HOLAR)  Inforce  Awards  Actuarial  Insurance Self Service  Insurance Unclaimed Liabilities  Insurance Online	Appraisal System Web Electronic Lender Identification  CONDO PUD Builder Centralized Property Tracking System Electronic Appraisal System  Web LGY  Access Manager  SAHSHA  VBA Data Warehouse Distribution of Operational Resources (DOOR)  Enterprise Wireless Messaging System (Blackberry) VBA Enterprise Messaging System  LGY Centralized Fax System  Review of Quality (ROQ)  Automated Sales Reporting (ASR)  Electronic Card System (ECS)  Electronic Payroll Deduction (EPD)  Financial Management Information System (FMI)  Purchase Order Management System (POMS)  Veterans Canteen Web  Inventory Management System (IMS)  Synquest  RAI/MDS  ASSISTS  MUSE  Bbraun (CP Hemo)  VIC  BCMA Contingency Machines  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	BIRLS
Telecare Record Manager	Centralized Accounts Receivable System (CARS)
Omnicell	Compensation & Pension (C&P)
Powerscribe Dictation System	Corporate Database
EndoSoft	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	Master Veterans Record (MVR)
Spinal Bifida Program Ch 18	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) **ALL APPS CONTROLLED**

**AT THE FACILITY**

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

Title:	Name:	Phone:	Email:
Privacy Officer:	Garnett Best	202-461-7474	garnett.best@va.gov
Digital Signature Block			
Information Security Officer:	Craig Heitz	612-725-2132	craig.heiz@va.gov
Digital Signature Block			
Dr. James Laub Regional Director OI&T Region 1			
Chief Information Officer:		480-325-3131	james.laub@va.gov
Digital Signature Block			
Person Completing Document:	Craig Heitz	612-725-2132	craig.heiz@va.gov
Digital Signature Block			