

## (FY 2010) PIA: Final Signatures

Facility Name: Consolidated Mail Outpatient Pharmacy

Title:	Name:	Phone:	Email:
Privacy Officer:	LaRue Roberts	361-356-1269	larue.morian2@va.gov
Digital Signature Block			
Information Security Officer:	Yancy McPherson	843-745-8648	Yancy.McPherson@va.gov
Digital Signature Block			
Chief Information Officer:	Phil Burkhalter	520-209-3118	Phil.Burkhalter@va.gov
Digital Signature Block			
Person Completing Document:	LaRue Roberts	361-356-1269	larue.morian2@va.gov
Digital Signature Block			
System / Application / Program Manager:	John Burt	520-209-3117	John.Burt@va.gov
Digital Signature Block			

Date of Report: 11/18/2009  
Exhibit 300 - 029-00-02-00-01-  
OMB Unique Project Identifier 1120-00  
Program Office>VHA>VISN  
Project Name 00>Tucson CMOP>PBX

### **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 systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and

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: Program Office>VHA>VISN 00>Tucson CMOP>PBX

OMB Unique System / Application / Program Identifier (AKA: UPID #): Exhibit 300 - 029-00-02-00-01-1120-00

### Description of System / Application / Program:

The Consolidated Mail Outpatient Pharmacy has installed a Private Branch Exchange (PBX) System for telecommunication support of the program. The CMOP PBX System is a Siemens HiPath 3000 series telephone switch. The model number of the switch is a HiPath 3750 series telephone switch. The telephone switch consists of two rack mounted chassis that are providing distributed communications for the CMOP. The telephone switch has electrical protection in place to include the Uninterrupted Power Supply (UPS) system. The telephone switch is a Virtual Private Network to ensure security controls. The system is designed to be immune to computer viruses and the Management workstation has the latest virus scanning software with updated .dat files being installed automatically. The switch management workstation has the MS XP operating system with all latest patches mounted on this workstation. Logs for the system are maintained on a log server that is backed up each night. There are no telephone operators on this system. All calls are managed by a Automatic Call Distribution system. The Xpression server is an IBM server with the latest virus software installed and patches from Microsoft. Xpression server is also on the VPN for the telephone system. Access to this system is limited to the few individuals listed on the access list to the telephone switch room itself. All telephone equipment is mounted in a rack in the telephone switch room behind a lock and key, also with access controls in place on who has permission to access the facility. These system a do not store any patient data. Only data stored on the switch is the configuration of the telephone system itself no personal data is store.

Facility Name:	Consolidated Mail Outpatient Pharmacy		
<b>Title:</b>	<b>Name:</b>	<b>Phone:</b>	<b>Email:</b>
Privacy Officer:	LaRue Roberts	361-356-1269	<a href="mailto:larue.morian2@va.gov">larue.morian2@va.gov</a>
Information Security Officer:	Yancy McPherson	843-745-8648	<a href="mailto:Yancy.McPherson@va.gov">Yancy.McPherson@va.gov</a>
Chief Information Officer:	Phil Burkhalter	520-209-3118	<a href="mailto:Phil.Burkhalter@va.gov">Phil.Burkhalter@va.gov</a>
Person Completing Document:	LaRue Roberts	361-356-1269	<a href="mailto:larue.morian2@va.gov">larue.morian2@va.gov</a>
Other Titles:	John Burt	520-209-3117	<a href="mailto:John.Burt@va.gov">John.Burt@va.gov</a>
Other Titles:			
Other Titles:			
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	04/2008		
Date Approval To Operate Expires:	04/2011		

---

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

What is the expected number of individuals that will have their PII stored in this system: 0

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. 2008

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): 11/2009

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

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

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

## (FY 2010) PIA: System of Records

---

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

No

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)?

No

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?

No

Is a Privacy notice provided?

No

Proximity and Timing: Is the privacy notice provided at the time of data collection?

No

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 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)				
Family Relation (spouse, children, parents, grandparents, etc)				
Service Information				
Medical Information				
Criminal Record Information				
Guardian Information				
Education Information				
Benefit Information				
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)	No			
Family Relation (spouse, children, parents, grandparents, etc)	No			
Service Information	No			
Medical Information	No			
Criminal Record Information	No			
Guardian Information	No			
Education Information	No			
Benefit Information	No			
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					
Other Veteran Organization					
Other Federal Government Agency					
State Government Agency					
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? No

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

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

(FY 2010) PIA: Secondary Use

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

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: NA

How is data checked for completeness?

Answer: NA

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

Answer: NA

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

Answer: NA

*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: NA

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

Answer: NA

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

Answer: NA

Where are these procedures documented?

Answer: NA

How are data retention procedures enforced?

Answer: NA

Answer: NA No

*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: This system works in conjunction with strong authentication measures to ensure and authenticate the identification of VA network users. System interconnection agreement (SIA)s are a system level measure to ensure that all interconnected systems meet minimum VA access policies for interconnected systems from within and outside the VA wide area network (WAN) boundaries. Moreover, the VA employs a comprehensive incidence response unit to respond to unwanted incursions and institutes enterprise level ant-virus system to protect mission critical applications on the desktop. Finally, the VA security program is an iterative program with repeatable processes that, in an ongoing basis, will mitigate vulnerabilities, minimize security exposures and maintain security and operating risk at acceptable levels. NIST 800-53 security controls are in place and tested every three years or as needed.

---

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 checked="" 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 checked="" type="checkbox"/> Sabotage/Terrorism                    |
| <input checked="" type="checkbox"/> Communications Loss                  | <input checked="" type="checkbox"/> Storms/Hurricanes                     |
| <input checked="" type="checkbox"/> Computer Intrusion                   | <input checked="" type="checkbox"/> Substance Abuse                       |
| <input checked="" type="checkbox"/> Data Destruction                     | <input checked="" type="checkbox"/> Theft of Assets                       |
| <input checked="" type="checkbox"/> Data Disclosure                      | <input checked="" type="checkbox"/> Theft of Data                         |
| <input checked="" type="checkbox"/> Data Integrity Loss                  | <input checked="" type="checkbox"/> Vandalism/Rioting                     |
| <input checked="" type="checkbox"/> Denial of Service Attacks            | <input checked="" type="checkbox"/> Errors (Configuration and Data Entry) |
| <input type="checkbox"/> Earthquakes                                     | <input checked="" type="checkbox"/> Burglary/Break In/Robbery             |
| <input checked="" type="checkbox"/> Eavesdropping/Interception           | <input checked="" type="checkbox"/> Identity Theft                        |
| <input checked="" type="checkbox"/> Fire (False Alarm, Major, and Minor) | <input checked="" 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: None

---

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
- 

The controls are being considered for the project based on the selections from the previous assessments?  
The ultimate objective is to conduct the day-to-day operations of the VA and to accomplish our stated mission with what the Office of Management and Budget (OMB) Circular A-130 defines as adequate security including the magnitude of harm to individuals, the VA, or its assets resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow NIST SP800-53 low impact defined set of controls.

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

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)*

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

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

Minor app #1	Name		Description	Comments
		<input type="checkbox"/>	Is PII collected by this min or application?	
		<input type="checkbox"/>	Does this minor application store PII?	
			If yes, where?	
		Who has access to this data?		

Minor app #2	Name		Description	Comments
		<input type="checkbox"/>	Is PII collected by this min or application?	
		<input type="checkbox"/>	Does this minor application store PII?	
			If yes, where?	
		Who has access to this data?		

Minor app #3	Name		Description	Comments
		<input type="checkbox"/>	Is PII collected by this min or application?	
		<input type="checkbox"/>	Does this minor application store PII?	
			If yes, where?	
		Who has access to this data?		

---

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

Facility Name: Consolidated Mail Outpatient Pharmacy



Privacy Officer: LaRue Roberts 361-356-1269 larue.morian2@va.gov

LARUE A

Digital Signature Block

Digitally signed by: LARUE A ROBERTS  
 DN: CN = LARUE A ROBERTS O = Department of Veterans Affairs, Internal Staff  
 Date: 2009.12.21 13:57:36 -06'00

ROBERTS

Information Security Officer: Yancy McPherson 843-745-8648 Yancy.McPherson@va.gov

Digital Signature Block

Chief Information Officer: Phil Burkhalter 520-209-3118 Phil.Burkhalter@va.gov

Signature not verified!

Digital Signature Block

Digitally signed by: BURKHALTER, PHIL  
 DN: CN = BURKHALTER, PHIL O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff  
 Date: 2009.12.21 13:26:07'00  
 Reason: I am approving this document

Person Completing Document: LaRue Roberts 361-356-1269 larue.morian2@va.gov

LARUE A

Digital Signature Block

Digitally signed by: LARUE A ROBERTS  
 DN: CN = LARUE A ROBERTS O = Department of Veterans Affairs, Internal Staff  
 Date: 2009.12.21 13:57:48 -06'00

ROBERTS

System / Application / Program Manager: John Burt 520-209-3117 John.Burt@va.gov

Digital Signature Block

Date of Report: 11/18/2009

OMB Unique Project Identifier: Exhibit 300 - 029-00-02-00-01-

1120-00

Project Name: Program Office>VHA>VISN

00>Tucson CMQP>PBX