v. 2.00

Welcome to the PIA for FY 2013!

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.

Macros Must Be Enabled To Use Full Functionality For This Form Template!

Microsoft Office 2003: To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.
Or 1) When file opens click on Enable Macros at the prompt.

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.

Microsoft Office 2007: To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable All Macros; 2) Click OK

Microsoft Office 2010: To enable macros, go to: 1) File Tab > Options > Trust Center > Trust Center Settings > Macro Settings > Enable All Macros; 2) Click OK

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.

Final Signatures

Final signatures are required to be digitally signed; however wet signatures may be used on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.

Directions:

Privacy Impact Assessment Uploaded into SMART

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program.
If you find that you can't click on checkboxes, make sure that you are:

1) Not in "design mode" and

2) you have enabled macros.

All PIA Validation Letters should be mailed to PIAsupport@va.gov to receive full credit for submission.

INTERNAL WEBSITE : http://vaww.privacy.va.gov/PIA.asp

Various Privacy Data Websites:

EXTERNAL WEBSITE : http://www.privacy.va.gov/PRIVACY/Privacy_Impact_Assessment.asp

SORNs : http://www.rms.oit.va.gov/SOR_Records.asp

Directive Itself (6508): http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=414&FType=2

Roles and Responsibilities:

Schedule FY 2013 : http://www.privacy.va.gov/PRIVACY/Privacy_Impact_Assessment.asp

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 referenced in the procedure section of this document.

a. **Privacy Officer** is responsible for the overall coordination with their local Information Security Officers and system owners to review the PIA and ensure compliance with VA Directive 6508.

Please read the following guidance on when to submit a full PIA:
http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=527#page=10

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

c. **Information Technology (IT)** staff responsible for the privacy of the system data will perform a PIA in accordance with VA Directive 6508 and to immediately report all anomalies to the Privacy Service and appropriate management chain.

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

e. **Chief Information Officer (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)

Personally Identifiable Information (PII) is —any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Examples of PII include, but are not limited to:

- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Organizations should minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission.

A "routine use" is a Privacy Act discretionary authority published in the Federal Register that permits VA to disclose information or records from a Privacy Act-protected record without the patient's prior signed authorization. A "routine use" permits the:

(1) Release of PHI only when disclosure is also authorized by other applicable legal authorities, including 45 CFR Parts 160 and 164;

(2) Release of drug or alcohol abuse, HIV, or sickle cell anemia medical information only when the disclosure is also authorized by 38 U.S.C. 7332.		

(FY 2013) PIA: System Information	*Green Highlight = Must Answer Question		*Yellow Highlight = Required to Sign PIA
Program or System Name (as shown in SMART):	FPO>VHA>CMOP-TUCSON>LAN		
OMB Unique System / Application / Program Identifier (AKA: UPID #):	Exhibit 300-029-00-02-00-01-1120-00		
Description of System/ Application/ Program : "must match what is stated in System Security Plan (SSP)" ***Do not type more than allotted space!!!***	The Consolidated Mail Outpatient Pharmacy (CMOP) LAN establishes an interface for the electronic transfer of information between VHA Medical Centers (VAMCs) and the Consolidated Mail Outpatient Pharmacy host system for an integrated and highly automated outpatient prescription dispensing system. The CMOP LAN is used to transfer, process and manage the prescription data received from the medical center through the automated filling of the prescription.		
Facility or Program Office Name:	Consolidated Mail Outpatient Pharmacy (CMOP)		
Title:	**Name:**	**Phone:**	**Email:**
Privacy Officer:	LaRue Roberts	361-356-1269	larue.morian2@va.gov
Information Security Officer:	Paul Gillespie	708-786-7735	paul.gillespie@.va.gov
System Owner/Delegate:	Michael Quinn	919-383-7874 x238	michael.quinn@va.gov
Facility Chief Information Officer:*	Kelly Brooks	520-295-3446	kelly.brooks@va.gov
Information Owner:	Kenneth Siehr	913-758-4750	kenneth.siehr@va.gov
Other Titles:			
Person Completing Document:	LaRue Roberts	361-356-1269	larue.morian2@va.gov
Other Titles:			
Date of Last Full Approved PIA by VACO Privacy Services: (YYYY)			FY 2010
What specific legal authorities authorize this program or system:	7301		
What is the expected number of individuals that will have their PII stored in this system:			after RX filled and data transferred back to medical
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.			1995
Is there an authorized change control process which documents any changes to existing applications or systems?			◉ Yes ○ No ○ N/A : First PIA
If No, (Explain on Tab 8)			
Is there a contingency plan in place to process information when the system is down?			◉ Yes ○ No ○ N/A : First PIA
Has a PIA been completed within the last three years?			◉ Yes ○ No ○ N/A : First PIA
FISMA QUESTIONS			
Answers provided in this section must correspond with the FISMA information listed in SMART for this system.			
1. Is this a new system?	○ Yes ◉ No		
2. Does this system contain Federal information in identifiable form?	◉ Yes ○ No		

3. Does the system include information on the public?	(●) Yes ( ) No			
4. Is there a Privacy Impact Assessment (PIA) that covers this system?	(●) Yes ( ) No ( ) National Security System under 40 U.S.C. 11103, a PIA is not required for this system			
5. Is Federal-owned information in this system retrieved by name or unique identifier?	(●) Yes ( ) No			
6. What is the System of Records Notice (SORN) for this system?	121VA19			
7. Has this SORN been reviewed or updated within the last three years?	Yes last year			
Date of Report (MM/YYYY):			14-Nov-12	
Any check mark in the boxes below will require a full PIA. Please continue to the next TAB and complete the remaining questions.				
If there is no Personally Identifiable Information on your system , please complete TAB 2 & TAB 12. (See Comment for Definition of PII)				
☐ 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?				
Directions				

(FY 2013) PIA: System of Records

*Green Highlight = Must Answer Question

1. Is there a SORN (System of Records Notice) already in place?

(●) Yes ( ) No

***If Yes, select all of the appropriate SORN number(s) and continue to Tab 4:
***If No, continue to question 2

***Click to add. Delete SORN by highlighting SORN and comma if included and press the Delete key or place focus on area to delete all SORNs.

LIST OF SORN NUMBER(S) : 121VA19

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

2. If records are retrieved using any of the following entities, A SORN will be required
(Please check all that apply)

- [ ] Full Name
- [ ] Maiden Name
- [ ] Mother's Maiden Name
- [ ] Alias
- [ ] Social Security Number
- [ ] Passport Number
- [ ] Driver's License Number
- [ ] Taxpayer Identification Number
- [ ] Financial Account Number
- [ ] Credit Card Number
- [ ] Street Address
- [ ] Email Address
- [ ] Photographic Image
- [ ] Fingerprints
- [ ] Handwriting
- [ ] Other Biometric Data
- [x] Other (Explain on Tab 8)

3. Based on Question 2, is a SORN required?

(●) Yes ( ) No

***If Yes, has the process begun to obtain/acquire a SORN

(●) Yes ( ) No

Location where the specific applicable System of Records Notice may be accessed:

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

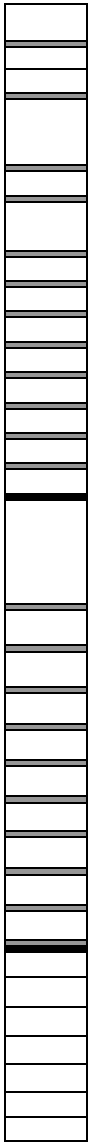
(FY 2013) PIA: Data Collection And Storage *Green Highlight = Must Answer Question

The Department of Veterans Affairs is actively trying to reduce the amount of personally identifiable information (PII) stored within its systems. Please do not collect more PII than what is required.

Please fill in each column for the data types selected.

Data Type	Collection Method	What are the subjects told about the intended use of their information?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	VA File Database	Healthcare	All	All
Family Relation (spouse, children, parents, grandparents, etc)	N/A	N/A	N/A	N/A
Service Information	N/A	N/A	N/A	N/A
Medical Information	VA File Database	Healthcare	All	All
Criminal Record Information	N/A	N/A	N/A	N/A
Guardian Information	N/A	N/A	N/A	N/A
Education Information	N/A	N/A	N/A	N/A
Benefit Information	N/A	N/A	N/A	N/A
Other (Explain on Tab 8)				

Data Type	Storage Method	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes / No	VA Files/Databases (Identify File)	Mandatory / Voluntary	Automated
Family Relation (spouse, children, parents, grandparents, etc)	Yes / No		Mandatory / Voluntary	
Service Information	Yes / No		Mandatory / Voluntary	
Medical Information	Yes / No	VA Files/Databases (Identify File)	Mandatory / Voluntary	Automated
Criminal Record Information	Yes / No		Mandatory / Voluntary	
Guardian Information	Yes / No		Mandatory / Voluntary	
Education Information	Yes / No		Mandatory / Voluntary	
Benefit Information	Yes / No		Mandatory / Voluntary	
Other (Explain on Tab 8)	Yes / No		Mandatory / Voluntary	
	(Please Select Yes/No)			
Proximity and Timing: Is the privacy notice provided at the time of data collection?	Yes / No			
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	Yes / No			
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	Yes / No			
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	Yes / No			
routine use(s)				



(FY 2013) PIA: Data Sharing *Green Highlight = Must Answer Question	** Any connection external to VA requires an ISA/MOU per VA 6500. This section below must be consistent with your System Security Plan Interconnection Security Agreement section.					
Organization	**Name of Agency/Organization**	**Do they access this system?**	**Identify the type of Data Sharing**	**Is PII or PHI Shared?**	**What is the procedure you reference for the release of information?**	
Internal Sharing: VA Organization	All Medical Centers	(•) Yes ( ) No	Healthcare	(•) Yes ( ) No	VHA Handbook 1605.2	
Other Veteran Organization		( ) Yes (•) No		( ) Yes (•) No		
Other Federal Government Agency	DOD and IHS	(•) Yes ( ) No	Healthcare	(•) Yes ( ) No	MOU	
State Government Agency		( ) Yes (•) No		( ) Yes (•) No		
Local Government Agency		( ) Yes (•) No		( ) Yes (•) No		
Research Entity		( ) Yes (•) No		( ) Yes (•) No		
☐ Other Project/ System (Explain on Tab 8)						
(FY 2013) PIA: Access to Records						
Does the system gather information from another system?	(•) Yes ( ) No					
Please enter the name of the system:		VHA Medical Centers VISTA Systems				
(FY 2013) PIA: Secondary Use						
Will PII data be included with any secondary use request?	( ) Yes (•) No	☐ Mental Health	☐ HIV	☐ Drug/Alcohol Counseling		
Check all that apply		☐ Sickle Cell	☐ Other (Explain on Tab 8)	☐ Research		

(FY 2013) PIA: Retention & Disposal *Green Highlight = Must Answer Question		
What is the data retention period?	RCS 10-1 link for VHA:	www.va.gov/vhapublications/rcs10/rcs10-1.pdf
Answer: CMOP Records are purged from the LAN Production Systems every 45 days. The data is maintained in a Centralized Database where records are purged in accordance to the RCS 10-1 for pharmacy records.	RCS VB-1, Part II Revised for VBA:	www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/part2.pdf
	National Archives and Records Administration:	www.nara.gov
Explain why the information is needed for the indicated retention period?		
Answer: Pharmaceutical care		
What are the procedures for eliminating data at the end of the retention period?		
Answer: Comply with VA regulations that address sanitization and disposal of VA data.		
Where are these procedures documented?		
Answer: VA Directive and Handbook 6500. NIST guidance.		
How are data retention procedures enforced?		
Answer: Through audit and monitoring to ensure staff is complying with VA regulations.		
Has the retention schedule been approved by the National Archives and Records Administration (NARA)		
(●) Yes ( ) No (Explain on Tab 8)		
(FY 2013) PIA: Children's Online Privacy Protection Act (COPPA)		
Will information be collected through the internet from children under age 13?		
( ) Yes (Explain on Tab 8) (●) No		

Answer:	Health Care Delivery

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 ( ) No (Explain on Tab 8)
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.	(•) Yes ( ) No (Explain on Tab 8)
Is security monitoring conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	(•) Yes ( ) No (Explain on Tab 8)
Is security assessment conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	(•) Yes ( ) No (Explain on Tab 8)
Is adequate physical security in place to protect against unauthorized access?	(•) Yes ( ) No (Explain on Tab 8)

*Ensure PE 2, PE-3, PE-6, PE-7, PE-8 have been addressed appropriately for your categorization

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

[✓] Biological Release	[✓] Fire	[✓] Lightning Strike	[✓] Terrorist
[✓] Blizzard	[✓] Flood	[✓] Malicious Code	[✓] Thunderstorm
[✓] Burglary/Break In	[✓] Hacker, Cracker	[✓] Password Privacy Negligence	[✓] Tornado
[✓] Civil Unrest	[✓] Hail	[✓] Personnel Unavailable	[ ] Tsunami
[✓] Component Failure	[✓] HAZMAT Release/Spill	[✓] Power Failure	[✓] User Negligence
[ ] Dam Failure	[✓] Human Health Emergency	[✓] Sabotage	[✓] User Sabotage
[ ] Dust/ Debris	[ ] Hurricane	[✓] System Intrusion, Break-Ins	[ ] Vibration
[ ] Earthquake	[✓] HVAC Failure	[✓] System Misconfiguration	[ ] Volcano
[✓] Extreme Cold	[ ] Indoor Humidity	[✓] System Penetration	[ ] Water Damage
[✓] Extreme Heat	[ ] Landslide	[✓] System Tampering	[✓] Winter Weather Hazards

*If any other risks identified, explain in Tab 8

Based upon the risks identified above, Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

[✓] Access Control	[✓] Configuration Management	[✓] Media Protection	[✓] System and Services Acquisition
[✓] Audit and Accountability	[✓] Contingency Planning	[✓] Personnel Security	[✓] System and Communication Protection
[✓] Awareness and Training	[✓] Identification and Authentication	[✓] Physical and Environmental Protection	[✓] System and Information Integrity
[✓] Security Assessment and Authorization	[✓] Incident Response	[✓] Risk Assessment	[✓] Planning [✓] Maintenance

Answer: (Other Controls) Explain on Tab 8

PIA: PIA Assessment

The PIA assessment is based on FIPS 199 which can be found within your system security plan (SSP).

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization? **(Choose One)**	( ) The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. ( ) The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. (•) The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? **(Choose One)**	(•) The potential impact is **high** if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. ( ) The potential impact is **moderate** if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals. ( ) The potential impact is **low** if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.
Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? **(Choose One)**	( ) The potential impact is **high** if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. (•) The potential impact is **moderate** if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals. ( ) The potential impact is **low** if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.

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.

(FY 2013) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

Tab 3 Row 24- At the medical center level data can be retrieved using patient name or social security number. At the CMOP level it can only be retrieved using a unique identifier assigned to the prescription when it is exported.

Tab 4 Row 30 - PSX CMOP Pharmacy Data File with patients name and address

Tab 4 Row 36 - PSX CMOP Pharmacy Data File with patients prescription data

(FY 2013) PIA: VBA Minor Applications

Which of these are sub-components of your system?

Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial	BCMA Contingency Machines	Automated Medical Information Exchange II (AIME II)
Agent Orange		Automated Medical Information System (AMIS)290
Appraisal System	Centralized Property Tracking System	Automated Standardized Performance Elements Nationwide (ASPEN)
ASSISTS	Common Security User Manager (CSUM)	Broome Closet
Awards	Compensation and Pension (C&P)	Centralized Accounts Receivable System (CARS)
Baker System	Control of Veterans Records (COVERS)	Committee on Waivers and Compromises (COWC)
Bbraun (CP Hemo)	Courseware Delivery System (CDS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
	Dental Records Manager	Compensation & Pension Training Website
	Education Training Website	
C&P Payment System	Electronic Appraisal System	Distribution of Operational Resources (DOOR)
C&P Training Website	Electronic Card System (ECS)	Educational Assistance for Members of the Selected Reserve Program CH 1606
CONDO PUD Builder	Electronic Payroll Deduction (EPD)	Electronic Performance Support System (EPSS)
	Eligibility Verification Report (EVR)	Enterprise Wireless Messaging System (Blackberry)
	Fiduciary Beneficiary System (FBS)	Financial Management Information System (FMI)
EndoSoft	Fiduciary STAR Case Review	Hearing Officer Letters and Reports System (HOLAR)
FOCAS	Financial and Accounting System (FAS)	Inquiry Routing Information System (IRIS)
Inforce	Insurance Unclaimed Liabilities	Modern Awards Process Development (MAP-D)
INS - BIRLS	Inventory Management System (IMS)	
Insurance Online	Interactive Voce Response (IVR)	Personal Computer Generated Letters (PCGL)
Insurance Self Service	LGY Centralized Fax System	Personnel Information Exchange System (PIES)
LGY Home Loans	Loan Service and Claims	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing	Loan Guaranty Training Website	Purchase Order Management System (POMS)
MES		Reinstatement Entitlement Program for Survivors (REAPS)
Mobilization	Mental Health Assistant	Reserve Educational Assistance Program CH 1607
Montgomery GI Bill	National Silent Monitoring (NSM)	RightFax
MUSE	Powerscribe Dictation System	Service Member Records Tracking System
Omnicell	Rating Board Automation 2000 (RBA2000)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Records Locator System	Systematic Technical Accuracy Review (STAR)
RAI/MDS	Remittance Processing System	Training and Performance Support System (TPSS)
Right Now Web	Review of Quality (ROQ)	VA Online Certification of Enrollment (VA-ONCE
SAHSHA	Search Participant Profile (SPP)	VA Reserve Educational Assistance Program
Script Pro	Spinal Bifida Program Ch 18	
SHARE	State Benefits Reference System	Veterans Assistance Discharge System (VADS)
Sidexis	State of Case/Supplemental (SOC/SSOC)	Veterans Exam Request Info System (VERIS)
Synquest	Telecare Record Manager	Veterans Insurance Claims Tracking and Response System (VICTARS)
	VBA Enterprise Messaging System	Veterans Service Representative (VSR) Advisor
VBA Training Academy		Vocational Rehabilitation & Employment (VR&E) CH 31
Veterans Canteen Web		
VETSNET Housekeeping	Web Electronic Lender Identification	Web Automated Folder Processing System (WAFPS)
		Web Automated Reference Material System (WARMS)
VR&E Training Website		Web Automated Verification of Enrollment
Web LGY		Web-Enabled Approval Management System (WEAMS)
		Web Service Medical Records (WebSMR)
		Work Study Management System (WSMS)

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

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

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

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

(FY 2013) PIA: VHA/NCA Minor Applications A-M				
Which of these are sub-components of your system?				
1184 Web	**Citrix**	**Embedded Fragment Registry**	**Incentive Awards**	
A4P	**Clinical Case Registries**	**ENCORE 2**	**Incident Reporting**	
ACCu Care	**Clinical Data Repository/Health Data Repository**	**ENDSOFT**	**Income Verification Match**	
ACCU Check	**Clinical Info Resource Network**	**Engineering**	**Incomplete Records Tracking**	
ACCU Med	**Clinical Monitoring System**	**Enrollment Application System**	**Inpatient Medications**	
Adobe Acrobat	**Clinical Notes Templates**	**Enterprise Terminology Server & VHA Enterprise Terminology Services**	**Intake/ Output**	
ADP Planning (PlanMan)	**Clinical Procedures**	**ePROMISE**	**Integrated Billing**	
ADT	**Clinical Reminders**	**Equipment/ Turn-in Request**	**Integrated Patient Funds**	
Adverse Reaction Tracking	**Clippership**	**Event Capture**	**Interim Management Support**	
Agent Cashier	**Combat Veteran Outreach**	**Event Driven Reporting**	**Inventory Management System**	
Air Fortress	**Committee on Waiver and Compromises**	**Extensible Editor**	**Kernal**	
ASISTS	**Consult/ Request Tracking**	**External Peer Review**	**Kids**	
Authorization/ Subscription	**Controlled Correspondence**	**EYECAP**	**KOWA**	
Auto Instrument	**Controlled Substances**	**Fee Based Claims System**	**Lab Service**	
Auto Replenishment/ Ward Stock	**CP&E**	**Fee Basis**	**Laboratory Electronic Data Interchange**	
AUTOCAD	**CPRS**	**Financial and Accounting System (FAS)**	**Letterman**	
Automated Access Request	**CPT/ HCPCS Codes**	**Financial Management System (FMS)**	**Lexicon Utility**	
Automated Info Collection Sys	**Credentials Tracking**	**Functional Independence**	**Library**	
Automated Lab Instruments	**Credit Card Authentication**	**Gen. Med. Rec. - I/O**	**List Manager**	
Automated Med Info Exchange	**Data Innovations**	**Gen. Med. Rec. - Vitals**	**Lynx Duress Alarm**	
Automated Sales Reporting	**DELIVEREX**	**Gen. Med.Rec. - Generator**	**Mailman**	
AutoMed	**Dental**	**GENDEX**	**MCCR National Database**	
Bad Code Med Admin	**DICTATION-Power Scribe**	**Generic Code Sheet**	**Meadows (MDWS)**	
Barcode Medication Administration Contingency Plan (BCU)	**Dietetics**	**Genesys**	**Medicine**	
BCMA Contingency Workstations	**Discharge Summary**	**Get Well Networks**	**Mental Health**	
BDN 301	**DRG Grouper**			
Beneficiary Travel	**DRM Plus**	**GMED**	**MHTP**	
BHL	**Drug Accountability**	**GRECC**	**MICOM**	
Big Fix	**DSIT**	**Health Data and Informatics**	**Microsoft Exchange E-mail System**	
CA Verified Components - DSSI	**DSS Extracts**	**Health Level Seven**	**Military/Vet Eye Injury Registry**	
Capacity Management - RUM	**DSS Quadramed**	**Health Summary**	**Minimal Patient Dataset**	
Capacity Management Tools	**EDS Whiteboard (AVJED)**	**Health Summary Contingency**	**Missing Patient Reg (Original) A4EL**	
CAPRI	**Education Tracking**	**HINQ**	**Mumps AudioFAX**	
Cardiff Teleform	**EEO Complaint Tracking**	**Hospital Based Home Care**	**MyHealthEVet**	
Cardiology Systems (stand alone servers from the network)	**EKG System**	**ICB**		
Care Management	**Electronic Card System (ECD)**	**ICR - Immunology Case Registry**		
CareTracker	**Electronic Payroll Deduction (EPD)**	**IFCAP**		
CHECKPOINT	**Electronic Signature**	**Imaging**		
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		CMOP PSX V2.0		
Description		Prescription Software		
Comments				
Is PII collected by this minor application?		YES		
Does this minor application store PII?		YES		
If yes, where?		PSX		
Who has access to this data?		Administrative Privileges needed		
Name				
Description				
Comments				
Is PII collected by this minor application?				
Does this minor application store PII?				
If yes, where?				
Who has access to this data?				
Name				
Description				
Comments				
Is PII collected by this minor application?				
Does this minor application store PII?				
If yes, where?				
Who has access to this data?				

(FY 2013) PIA: VHA/NCA Minor Applications N-Z

Which of these are sub-components of your system?

National Cemetery Association	**Pharmacy Data Management**	**Scanning Exam and Evaluation System**	**VBECS**
National Drug File	**Pharmacy National Database**	**Scheduling**	**VDEF**
National Laboratory Test	**Pharmacy Prescription Practice**	**Security Suite Utility Pack**	**Vendor - Document Storage Sys**
NDBI	**PICIS OR**	**Sentillion**	**Veterans Canteen Web**
Network Health Exchange	**Police & Security**	**Shift Change Handoff Tool**	**Veterans Information Solution**
NOAHLINK	**Problem List**	**ShoreTel**	**VHAHUNAPP1**
NOIS	**Progress Notes**	**Social Work**	**VHAHUNFPC1**
Nursing Service	**Prosthetics**	**Stellant**	**VHS & RA Tracking System**
Occurrence Screen	**Purchase Order Management System**	**Stentor**	**Visit Tracking**
Omnicell	**Pyxis**	**Surgery**	**VISTA RAD**
Oncology	**Q-Matic**	**Survey Generator**	**VISTA RO**
Onvicord (VLOG)	**QMSI Prescription Processing**	**Telecare Record Manager**	**VistALink**
Optifill	**Quality Assurance Integration**	**Temp Trak**	**VistALink Security**
Order Entry/ Results Reporting	**Quality Improvement Checklist**	**Text Integration Utilities**	**Visual Impairment Service Team ANRV**
Outpatient Pharmacy	**QUASER**	**Tickler Database**	**Vitria BusinessWare**
P2000 ROBOT	**Radiology/ Nuclear Medicine**	**Toolkit**	**VIXS**
PACS database	**RAFT**	**TopCon**	**Voluntary Timekeeping**
Patch Module	**RALS**	**TraceMaster**	**Voluntary Timekeeping National**
Patient Data Exchange	**Record Tracking**	**Tracking Continuing Education**	**WEB HINQ**
Patient Feedback	**Registration**	**Traumatic Brain Injury**	**Whiteboard**
Patient Representative	**Release of Information - DSSI**	**Unwinder**	**Women's Health**
PCE Patient Care Encounter	**Remote Order/ Entry System**	**Utility Management Rollup**	**Workload and Overtime**
Personal Computer Generated Letters	**RPC Broker**	**Utilization Review**	
Pharmacy Benefits Management	**Run Time Library**	**VA Conference Room Registration**	
	SAGG	**VA Fileman**	
	SAN	**VAMedSafe**	

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

Name	
Description	
Comments	
Is PII collected by this minor application?	
Does this minor application store PII?	
If yes, where?	
Who has access to this data?	

Name	
Description	
Comments	
Is PII collected by this minor application?	
Does this minor application store PII?	
If yes, where?	
Who has access to this data?	

Name	
Description	
Comments	
Is PII collected by this minor application?	
Does this minor application store PII?	
If yes, where?	
Who has access to this data?	

(FY 2013) PIA: Final Signatures *Green Highlight = Must Answer Question

Facility Name:	Consolidated Mail Outpatient Pharmacy (CMOP)		
Title:	Name:	Phone:	Email:
Privacy Officer:	LaRue Roberts	361-356-1269	larue.morian2@va.gov
Digital Signature Block			
Information Security Officer:	John McKinley	913-758-4741	john.mckinley@va.gov
Digital Signature Block			
System Owner/Delegate:	Michael Quinn	919-383-7874 x238	michael.quinn@va.gov
Digital Signature Block			
Facility Chief Information Officer	Kelly Brooks	520-295-3446	kelly.brooks@va.gov
Digital Signature Block			
Information Owner:	Kenneth Siehr	913-758-4750	kenneth.siehr@va.gov
Digital Signature Block			
Other Titles:			
Digital Signature Block			
Date of Report:	14-Nov-12		
OMB Unique Project Identifier	Exhibit 300-029-00-02-00-01-1120-00		
Project Name	FPO>VHA>CMOP-TUCSON>LAN		

The Signature Process:

• Complete the PIA form.

• Name the PIA Excel FORM [“FY13-Region # - Facility Name - Facility # -Date(mmddyyyy).xls”]

• Example: “FY13-Region3-Lexington VAMC-596-10302008.xls”

• Submit the completed PIA Excel form to SMART Database.

• Fix errors the reviewers sent back, rename the file and submit to SMART Database

• If no errors, convert form into PDF with Nuance PDF Professional.

• Name the PIA PDF form [“FY13-Region #-Facility Name- Facility # -Date(mmddyyyy).xls”]

• Obtain digital signatures on the “Final Signatures tab”

• Submit signed PIA PDF form to the SMART Database.