

Welcome to the PIA for FY 2012!	
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 <u>Enable Macros at the prompt.</u> Or 1) When file opens click on <u>Enable Macros at the prompt.</u>
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
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 digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.
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 Christina.Pettit@va.gov to receive full credit for submission.
INTERNAL WEBSITE : http://vawww.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&FTType=2
Roles and Responsibilities:	Schedule FY 2012 : 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 and review of the PIA to ensure compliance with VA Directive 6508	
b. Records Officer is responsible for supplying records retention and deletion schedules	
c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Directive 6508 and to immediately report all anomalies to the Privacy Service and appropriate management chain.	
d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.	
e. 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	
• 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 2012) PIA: System Information		*Green Highlight = Must Answer Question	*Yellow Highlight = Required to Sign PIA
Program or System Name (as shown in SMART):	Region 1 > VHA > VISN 22 > Greater Los Angeles HCS (West LA) > LAN		
OMB Unique System / Application / Program Identifier (UPID #):	(AKA: 029-00-02-00-01-1120-00		
Description of System/ Application/ Program : "must match what is stated in System Security Plan (SSP)"	The VA GLAHS LAN provides internal and external network connectivity for users to access major VA applications. Major applications include VISTA/CPRS, Windows 2003 Active Directory, Microsoft Exchange application and database servers, PACs, Vista Imaging, and EAS. Non-major applications that support the facility include: word		
Facility or Program Office Name:	VA Greater Los Angeles Healthcare System		
Title:	Name:	Phone:	Email:
Privacy Officer:	Jenelle Happy	(310) 478-7711 ext 41	Jenelle.Happy@va.gov
Information Security Officer:	Dewitt Sanders	(818) 891-7711 ext 78	Dewitt.Sanders@va.gov
System Owner/Delegate:	Jack Seymour	(303) 504-2686	Jack.Seymour@va.gov
Chief Information Officer:	Eugene Archey	(818) 895-9448	Eugene.Archey@va.gov
Information Owner:			
Other Titles:			
Person Completing Document:	Dewitt Sanders	(818) 891-7711 ext 78	Dewitt.Sanders@va.gov
Other Titles:			
Date of Last Full Approved PIA by VACO Privacy Services: (MM/YYYY)			07/2008
What specific legal authorities authorize this program or system:	Title 38 , United States Code, section		
What is the expected number of individuals that will have their PII stored in this system: 0			5000 +
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.	1978		
Is there an authorized change control process which documents any changes to existing applications or systems?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> 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?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PIA		
Has a PIA been completed within the last three years?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PIA		
FISMA QUESTIONS			
1. Is this a new system?	<input type="radio"/> Yes <input checked="" type="radio"/> No		
2. Does this system contain Federal information in identifiable form?	<input checked="" type="radio"/> Yes <input type="radio"/> No		
3. Does the system include information on the public?	<input type="radio"/> Yes <input checked="" type="radio"/> No		
4. Is there a Privacy Impact Assessment (PIA) that covers this system?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> 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	<input checked="" type="radio"/> Yes <input type="radio"/> No		
6. What is the System of Records Notice (SORN) for this system?	24VA19		
7. Has this SORN been reviewed or updated within the last three years?	Yes in 2009		
Date of Report (MM/YYYY):	1-Oct-11		
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)			
<input type="checkbox"/>	Have any changes been made to the system since the last PIA?		
<input type="checkbox"/>	Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?		
<input checked="" type="checkbox"/>	Will this system/application/program retrieve information on the basis of name, unique identifier, symbol or other PII data?		
<input checked="" type="checkbox"/>	Does this system/application/program collect, store, or disseminate PII/PHI data?		
<input checked="" type="checkbox"/>	Does this system/application/program collect, store or disseminate the SSN?		
Directions			

(FY 2012) PIA: System of Records

*Green Highlight = Must Answer Question

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

<input checked="" type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> Not Sure
<input checked="" type="radio"/> Yes	<input type="radio"/> No	

***If Yes, select all of the appropriate SORN number(s):
 ***If Not Sure, continue to question 3

***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) :

24VA19

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

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

<input checked="" type="checkbox"/> Full Name
<input type="checkbox"/> Maiden Name
<input type="checkbox"/> Mother's Maiden Name
<input type="checkbox"/> Alias
<input checked="" type="checkbox"/> Social Security Number
<input type="checkbox"/> Passport Number
<input type="checkbox"/> Driver's License Number
<input type="checkbox"/> Taxpayer Identification Number
<input type="checkbox"/> Financial Account Number
<input type="checkbox"/> Credit Card Number
<input type="checkbox"/> Street Address
<input type="checkbox"/> Email Address
<input type="checkbox"/> Photographic Image
<input type="checkbox"/> Fingerprints
<input type="checkbox"/> Handwriting
<input type="checkbox"/> Other Biometric Data
<input type="checkbox"/> Other (Explain on Tab 8)

- 4. Based on Question 3, is a SORN required?

<input checked="" type="radio"/> Yes	<input type="radio"/> No
<input checked="" type="radio"/> Yes	<input type="radio"/> No

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

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

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

(FY 2012) PIA: Data Collection And Storage				
*Green Highlight = Must Answer Question				
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)	Paper & Electronic	Collection is for treatment, payment, healthcare operations, and VA Benefits; Notice of Privacy Practices; Federal Register Public Notice of Routine Uses, Storage, Retrievability, Safeguards, Retention and Disposal, Notification period, System Managers and Address, Notification, Access and Contesting Procedure, Record Source Categories.	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	Paper & Electronic	Collection is for treatment, payment, healthcare operations, and VA Benefits;	Written	Written
Service Information	Paper & Electronic	Collection is for treatment, payment, healthcare operations, and VA Benefits; Notice of Privacy Practices; Federal Register Public Notice of Routine Uses, Storage, Retrievability, Safeguards, Retention and Disposal, Notification period, System Managers and Address, Notification, Access and Contesting Procedure, Record Source Categories.	Written	Written
Medical Information	Paper & Electronic	Collection is for treatment, payment, healthcare operations, and VA Benefits; Notice of Privacy Practices; Federal Register Public Notice of Routine Uses, Storage, Retrievability, Safeguards, Retention and Disposal, Notification period, System Managers and Address, Notification, Access and Contesting Procedure, Record Source Categories.	Written	Written
Criminal Record Information	ALL	Collection is for treatment, payment, healthcare operations, and VA Benefits; Notice of Privacy Practices; Federal Register Public Notice of Routine Uses, Storage, Retrievability, Safeguards, Retention and Disposal, Notification period, System Managers and Address, Notification, Access and Contesting Procedure, Record Source Categories.	Written	Written

(FY 2012) PIA: Data Sharing		** 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.			
*Green Highlight = Must Answer Question					
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	VHA; VBA; NCA; OIG; OGC	<input checked="" type="radio"/> Yes <input type="radio"/> No	Treatment, payment, benefits, and healthcare operations; Legal Representation; Law Enforcement; Adjudication of Claims; VA Benefits	<input checked="" type="radio"/> Yes <input type="radio"/> No	VHA Handbook 1605.1; Standing Letter Agreements
Other Veteran Organization	VSO	<input checked="" type="radio"/> Yes <input type="radio"/> No	Medical and Benefit and Healthcare information for veteran benefit assistance	<input type="radio"/> Yes <input checked="" type="radio"/> No	VHA Handbook 1605.1; Patient Authorization
Other Federal Government Agency	VHA; VBA; SSA; DOD; DOJ; FDA	<input checked="" type="radio"/> Yes <input type="radio"/> No	Treatment, payment, benefits, and healthcare operations	<input checked="" type="radio"/> Yes <input type="radio"/> No	VHA Handbook 1605.1; .1: Sharing Agreements; Business Associate Agreements; Standing Letters; Health and Safety
State Government Agency	State of California, California Department of Public Health; Medical Board of California; California State Veteran Homes; Organ Procurement Organization	<input type="radio"/> Yes <input checked="" type="radio"/> No	Health and Safety; Criminal Activity; Donor Purposes	<input checked="" type="radio"/> Yes <input type="radio"/> No	VHA Handbook 1605.1; Sharing Agreements; Contracts
Local Government Agency	Law Enforcement Agencies	<input checked="" type="radio"/> Yes <input type="radio"/> No	Health and Safety; Criminal Activity	<input checked="" type="radio"/> Yes <input type="radio"/> No	VHA Handbook 1605.1; Standing Letter Agreements
Research Entity	USC, UCLA Affiliates	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	VHA Handbook 1605.1; Patient Authorization; Patient Care Referrals for Healthcare; Affiliate Agreement
<input type="checkbox"/> Other Project/ System (Explain on Tab 8)					
(FY 2012) PIA: Access to Records					
Does the system gather information from another system?		<input checked="" type="radio"/> Yes <input type="radio"/> No			
Please enter the name of the system:					
(FY 2012) PIA: Secondary Use					
Will PII data be included with any secondary use request?		<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="checkbox"/> Mental Health	<input type="checkbox"/> HIV	<input type="checkbox"/> Drug/Alcohol Counseling
Check all that apply			<input type="checkbox"/> Sickle Cell	<input type="checkbox"/> Other (Explain on Tab 8)	<input type="checkbox"/> Research

(FY 2012) PIA: Records Management		*Green Highlight = Must Answer Question	
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?			
<input type="radio"/> Yes (Explain on Tab 8) <input checked="" type="radio"/> No			
Is the data collected to only what is necessary to provide requested service?			
<input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8)			
Has the data provided been verified as complete?			
<input checked="" type="checkbox"/> Veteran Verified <input type="checkbox"/> Received From Database <input type="checkbox"/> Verification Unknown			
(FY 2012) PIA: Retention & Disposal			
What is the data retention period?		RCS 10-1 link for VHA: www.va.gov/vhapublications/rcs10/rcs10-1.pdf	
75 Years		RCS VB-1, Part II Revised for VBA: www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/part2.pdf	
		National Archives and Records Administration: w.nara.gov	
Explain why the information is needed for the indicated retention period?			
Answer: Health care			
What are the procedures for eliminating data at the end of the retention period?			
Answer: In accordance with disposition instructions in the NARA records schedule contained in FILES 203, the NARA Files			
Where are these procedures documented?			
Answer: RC10-1			
How are data retention procedures enforced?			
Answer: The Health Information Resource Service is responsible for developing policies and procedures			
Has the retention schedule been approved by the National Archives and Records Administration (NARA)			
<input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8)			
(FY 2012) PIA: Children's Online Privacy Protection Act (COPPA)			
Will information be collected through the internet from children under age 13?			
<input type="radio"/> Yes (Explain on Tab 8) <input checked="" type="radio"/> No			

(FY 2012) PIA: Security *Green Highlight = Must Answer Question

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	<input checked="" type="radio"/> Yes	<input type="radio"/> 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..	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Is security monitoring conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Is security assessment conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Is adequate physical security in place to protect against unauthorized access?	<input checked="" type="radio"/> Yes	<input type="radio"/> 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)

<input checked="" type="checkbox"/> Biological Release	<input checked="" type="checkbox"/> Fire	<input type="checkbox"/> Lightning Strike	<input checked="" type="checkbox"/> Terrorism
<input type="checkbox"/> Blizzard	<input checked="" type="checkbox"/> Flood	<input checked="" type="checkbox"/> Malicious Code	<input type="checkbox"/> Thunderstorm
<input checked="" type="checkbox"/> Burglary/Break In	<input checked="" type="checkbox"/> Hacker, Cracker	<input checked="" type="checkbox"/> Password Privacy Negligence	<input type="checkbox"/> Tornado
<input checked="" type="checkbox"/> Civil Unrest	<input type="checkbox"/> Hail	<input checked="" type="checkbox"/> Personnel Unavailable	<input type="checkbox"/> Tsunami
<input checked="" type="checkbox"/> Component Failure	<input checked="" type="checkbox"/> HAZMAT Release/Spill	<input type="checkbox"/> Power Failure	<input checked="" type="checkbox"/> User Negligence
<input type="checkbox"/> Dam Failure	<input checked="" type="checkbox"/> Human Health Emergency	<input type="checkbox"/> Sabotage	<input checked="" type="checkbox"/> User Sabotage
<input type="checkbox"/> Dust/Debris	<input type="checkbox"/> Hurricane	<input checked="" type="checkbox"/> System Intrusion, Break-Ins	<input checked="" type="checkbox"/> Vibration
<input checked="" type="checkbox"/> Earthquake	<input checked="" type="checkbox"/> HVAC Failure	<input checked="" type="checkbox"/> System Misconfiguration	<input type="checkbox"/> Volcano
<input type="checkbox"/> Extreme Cold	<input type="checkbox"/> Indoor Humidity	<input checked="" type="checkbox"/> System Penetration	<input checked="" type="checkbox"/> Water Damage
<input checked="" type="checkbox"/> Extreme Heat	<input type="checkbox"/> Landslide	<input checked="" type="checkbox"/> System Tampering	<input type="checkbox"/> 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)

<input checked="" type="checkbox"/> Access Control	<input checked="" type="checkbox"/> Configuration Management	<input checked="" type="checkbox"/> Media Protection	<input checked="" type="checkbox"/> System and Services Acquisition
<input checked="" type="checkbox"/> Audit and Accountability	<input checked="" type="checkbox"/> Contingency Planning	<input checked="" type="checkbox"/> Personnel Security	<input checked="" type="checkbox"/> System and Communication Protection
<input checked="" type="checkbox"/> Awareness and Training	<input checked="" type="checkbox"/> Identification and Authentication	<input checked="" type="checkbox"/> Physical and Environmental Protection	<input checked="" type="checkbox"/> System and Information Integrity
<input checked="" type="checkbox"/> Security Assessment and Authorization	<input checked="" type="checkbox"/> Incident Response	<input checked="" type="checkbox"/> Risk Assessment	<input checked="" type="checkbox"/> Planning
			<input checked="" type="checkbox"/> Maintenance

Answer: (Other Controls) Explain on Tab 8

PIA: PIA Assessment

Based upon NIST 800-60, volume II; List the Information data types chosen as a basis for your FIPS 199 System Categorization.

	Healthcare Delivery Services Information
<p>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)</p>	<input type="checkbox"/> 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. <input type="checkbox"/> The potential impact is moderate if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. <input checked="" type="checkbox"/> The potential impact is low if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
<p>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)</p>	<input checked="" type="checkbox"/> 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. <input type="checkbox"/> The potential impact is moderate if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> The potential impact is low if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.
<p>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)</p>	<input type="checkbox"/> 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. <input type="checkbox"/> The potential impact is moderate if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals. <input checked="" type="checkbox"/> 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 2012) 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.

(FY 2012) PIA: VBA Minor Applications

Which of these are sub-components of your system? N/A		
	Access Manager	Automated Sales Reporting (ASR)
	Actuarial	Automated Folder Processing System (AFPS)
	Agent Orange	Automated Medical Information Exchange II (AIME II)
	Appraisal System	Automated Medical Information System (AMIS)290
	ASSISTS	Automated Standardized Performance Elements Nationwide (ASPEN)
	Awards	Broome Closet
	Baker System	Centralized Accounts Receivable System (CARS)
	Bbraun (CP Hemo)	Committee on Waivers and Compromises (COWC)
	C&P Payment System	Compensation and Pension (C&P) Record Interchange (CAPRI)
	C&P Training Website	Compensation & Pension Training Website
	CONDO PUD Builder	Distribution of Operational Resources (DOOR)
	EndoSoft	Educational Assistance for Members of the Selected Reserve Program CH 1606
	FOCAS	Electronic Appraisal System
	Inforce	Electronic Card System (ECS)
	INS - BIRLS	Electronic Payroll Deduction (EPD)
	Insurance Online	Electronic Performance Support System (EPSS)
	Insurance Self Service	Eligibility Verification Report (EVR)
	LGV Home Loans	Enterprise Wireless Messaging System (Blackberry)
	LGV Processing	Fiduciary Beneficiary System (FBS)
	MES	Financial Management Information System (FMI)
	Mobilization	Fiduciary STAR Case Review
	Montgomery GI Bill	Hearing Officer Letters and Reports System (HOLAR)
	MUSE	Inquiry Routing Information System (IRIS)
	Omnicell	Financial and Accounting System (FAS)
	Priv Plus	Inforce Insurance Unclaimed Liabilities
	RAI/MDS	Inventory Management System (IMS)
	Right Now Web	Modern Awards Process Development (MAP-D)
	SAHSHA	Interactive Voce Response (IVR)
	Script Pro	Personal Computer Generated Letters (PCGL)
	SHARE	Personnel Information Exchange System (PIES)
	Sidexis	Loan Service and Claims
	Synquest	Loan Guaranty Training Website
	VBA Training Academy	Purchase Order Management System (POMS)
	Veterans Canteen Web	Reinstatement Entitlement Program for Survivors (REAPS)
	VETSNET Housekeeping	Reserve Educational Assistance Program CH 1607
	VR&E Training Website	National Silent Monitoring (NSM)
	Web LGY	RightFax
		Powerscribe Dictation System
		Service Member Records Tracking System
		Rating Board Automation 2000 (RBA2000)
		Survivors and Dependents Education Assistance CH 35
		Records Locator System
		Systematic Technical Accuracy Review (STAR)
		Remittance Processing System
		Training and Performance Support System (TPSS)
		Review of Quality (ROQ)
		VA Online Certification of Enrollment (VA-ONCE)
		Search Participant Profile (SPP)
		VA Reserve Educational Assistance Program
		Spinal Bifida Program Ch 18
		State Benefits Reference System
		Veterans Assistance Discharge System (VADS)
		State of Case/Supplemental (SOC/SSOC)
		Veterans Exam Request Info System (VERIS)
		Telecare Record Manager
		Veterans Insurance Claims Tracking and Response System (VICTARS)
		Veterans Service Representative (VSR) Advisor
		VBA Enterprise Messaging System
		Vocational Rehabilitation & Employment (VR&E) CH 31
		Web Electronic Lender Identification
		Web Automated Folder Processing System (WAFFPS)
		Web Automated Reference Material System (WARMS)
		Web Automated Verification of Enrollment
		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 2012) PIA: Minor Applications A-M

Which of these are sub-components of your system?				
X	1184 Web		X	Electronic Signature
	A4P			Imaging
		X		Incentive Awards
X	ACCu Care	X		Incident Reporting
			X	Income Verification Match
X	ACCU Check			Incomplete Records Tracking
		X		Inpatient Medications
X	ACCU Med	X		Intake/ Output
			X	Integrated Billing
X	Adobe Acrobat			Integrated Patient Funds
		X		Interim Mangement Support
	ADP Planning (PlanMan)	X		Inventory Management System
			X	Kernal
		X		Kids
	ADT	X		KOWA
			X	Lab Service
	Adverse Reaction Tracking		X	Laboratory Electronic Data Interchange
		X		Letterman
X	Agent Cashier			Lexicon Utility
		X		Library
X	Air Fortress			List Manager
		X		Lynx Duress Alarm
X	ASISTS	X		Mailman
			X	MCCR National Database
X	Authorization/ Subscription	X		Meadows (MDWS)
			X	Medicine
X	Auto Instrument	X		Mental Health
		X		MHPT
	Auto Replenishment/ Ward Stock		X	MICOM
		X		Microsoft Exchange E-mail System
X	AUTOCAD	X		Military/Vet Eye Injury Registry
			X	Minimal Patient Dataset
	Automated Access Request	X		Missing Patient Reg (Original) A4EL
		X		Mumps AudioFAX
	Automated Info Collection Sys	X		MyHealthEvet
		X		
X	Automated Lab Instruments	X		
			X	
X	Automated Med Info Exchange	X		
		X		
X	Automated Sales Reporting	X		
		X		
X	AutoMed	X		
			X	
	Bad Code Med Admin		X	
		X		
X	Barcode Medication Administration Contingency Plan (BCU)	X		
			X	
X	BCMA Contingency Workstations			
		X		
	BDN 301		X	
		X		
X	Beneficiary Travel	X		
		X		
X	Big Fix	X		
		X		
X	CA Verified Components - DSSI	X		
		X		
	Capacity Management - RUM	X		
		X		
X	Capacity Management Tools	X		
		X		
X	CAPRI	X		
		X		
	Cardiff Teleform	X		
		X		
X	Cardiology Systems (stand alone servers from the network)	X		
		X		
X	Care Management	X		
		X		
X	CareTracker	X		
		X		
	CHECKPOINT	X		
		X		
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 2012) PIA: Final Signatures		*Green Highlight = Must Answer Question	
Facility Name:	VA Greater Los Angeles Healthcare System		
Title:	Name:	Phone:	Email:
Privacy Officer:	Jenelle Happy	(310) 478-7711 ext 41513	Jenelle.Happy@va.gov
Information Security Officer:	Dewitt Sanders	ext 7865	Dewitt.Sanders@va.gov
System Owner/Delegate:	Jack Seymour	(303) 504-2686	Jack.Seymour@va.gov
Chief Information Officer:	Eugene Archey	(818) 895-9448	Eugene.Archey@va.gov
Other Titles:	0	0	0
Digital Signature Block			
Date of Report:	1-Oct-11		
OMB Unique Project Identifier	029-00-02-00-01-1120-00		
Project Name	Region 1 > VHA > VISN 22 > Greater Los Angeles HCS (West LA) > LAN		
<p>The Signature Process:</p> <ul style="list-style-type: none"> • Complete the PIA form. • Name the PIA Excel FORM ["FY12-Region # - Facility Name - Facility # -Date(mmddyyyy).xls"] <ul style="list-style-type: none"> • Example: "FY12-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 <ul style="list-style-type: none"> • If no errors, convert form into PDF with Nuance PDF Professional. • Name the PIA PDF form ["FY12-Region #-Facility Name- Facility # -Date(mmddyyyy).xls"] <ul style="list-style-type: none"> • Obtain digital signatures on the "Final Signatures tab" • Submit signed PIA PDF form to the SMART Database. 			