

<u>Welcome to the PIA for FY 2012!</u>		
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.		<u>Macros Must Be Enabled To Use Full Functionality For This Form Template!</u>
		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&FTYPE=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 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 2012) PIA: System Information		*Green Highlight = Must Answer Question		*Yellow Highlight = Required to Sign PIA	
Program or System Name (as shown in SMART):		Region1/VHA/VISN21/ San Francisco VAMC/ Local Area Network (LAN)			
OMB Unique System / Application / Program Identifier (AKA: UPID #):		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!!***		<p>The Windows 2003 Local Area Network (LAN) system is comprised of workstations, servers, printers and other equipment which include devices such as routers, hubs, switches, and firewalls that support communications to extended LAN locations such as community based outpatient clinics (CBOC's). The LAN system also includes subsystem components such as tape drives, disk drives, uninterruptible power supplies (UPS), network area storage (NAS), and storage access networks (SAN). Within this plan each facility will document their own physical description of their LAN system including local and extended LAN locations, its components and subsystems. The LAN infrastructure does not contain any Personally Identifiable Information. This information exists on the file servers of the LAN.</p>			
Facility or Program Office Name:		San Francisco VA Medical Center			
Title:		Name:		Phone:	
Privacy Officer:		Elaine Tran		415-221-4810 x2135	
Information Security Officer:		Dennis Lawton		415-221-4810 x2141	
System Owner/Delegate:		Judith Ringler		415-221-4810 x6968	
Chief Information Officer:		Judith Ringler		415-221-4810 x6968	
Information Owner:		Judith Ringler		415-221-4810 x6968	
Other Titles:					
Person Completing Document:		Elaine Tran		415-221-4810 x2135	
Other Titles:					
Date of Last Full Approved PIA by VACO Privacy Services: (MM/YYYY)				04/2009	
What specific legal authorities authorize this program or system:		79VA19			
What is the expected number of individuals that will have their PII stored in this system:				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.				Approximately 20 years.	
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 checked="" type="radio"/> Yes <input 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 identifier?	<input checked="" type="radio"/> Yes <input type="radio"/> No			
6. What is the System of Records Notice (SORN) for this system?	79VA19			
7. Has this SORN been reviewed or updated within the last three years?	Yes three years ago			
Date of Report (MM/YYYY):			04/2012	
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 checked="" type="checkbox"/>	Have any changes been made to the system since the last PIA?			
<input checked="" 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?

Yes No Not Sure

Yes 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) :

79VA19
RCS 10-1

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

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

Yes No

Yes 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)	ALL	Depending upon job responsibilities of any given employee, they may store PII/PHI on VA Servers for Department use.	All	All
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Depending upon job responsibilities of any given employee, they may store PII/PHI on VA Servers for Department use.	All	All
Service Information	ALL	Depending upon job responsibilities of any given employee, they may store PII/PHI on VA Servers for Department use.	All	All
Medical Information	ALL	Depending upon job responsibilities of any given employee, they may store PII/PHI on VA Servers for Department use.	All	All
Criminal Record Information	ALL	This information is only available in HRMS Department and used for Personnel, Investigatory and Contracting Purposes	All	All
Guardian Information	ALL	Depending upon job responsibilities of any given employee, they may store PII/PHI on VA Servers for Department use.	All	All
Education Information	ALL	Depending upon job responsibilities of any given employee, they may store PII/PHI on VA Servers for Department use.	All	All
Benefit Information	ALL	Depending upon job responsibilities of any given employee, they may store PII/PHI on VA Servers for Department use.	All	All
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)	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input type="radio"/> Voluntary
Family Relation (spouse, children, parents, grandparents, etc)	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input type="radio"/> Voluntary
Service Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input type="radio"/> Voluntary
Medical Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input type="radio"/> Voluntary
Criminal Record Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary
Guardian Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input type="radio"/> Voluntary

Education Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary	
Benefit Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary	
Other (Explain on Tab 8)	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary	
	<i>(Please Select Yes/No)</i>			
Proximity and Timing: Is the privacy notice provided at the time of data collection?	<input checked="" type="radio"/> Yes <input type="radio"/> No			
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	<input checked="" type="radio"/> Yes <input type="radio"/> No			
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	<input checked="" type="radio"/> Yes <input type="radio"/> No			
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	<input checked="" type="radio"/> Yes <input type="radio"/> No			
	routine use(s)			

(FY 2012) 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	VBA/VHA/MPI/HEC	<input checked="" type="radio"/> Yes <input type="radio"/> No	Benefits and Research	<input checked="" type="radio"/> Yes <input type="radio"/> No	VHA Handbook 1605.2	
Other Veteran Organization	VSO	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran's	<input checked="" type="radio"/> Yes <input type="radio"/> No	HIPAA Authorization/Waiver	
Other Federal Government Agency	SSA/DOD/DOJ/HHS/OIG	<input checked="" type="radio"/> Yes <input type="radio"/> No	Healthcare	<input checked="" type="radio"/> Yes <input type="radio"/> No	VHA Handbook 1605.2	
State Government Agency	CPS, Tumor Board	<input checked="" type="radio"/> Yes <input type="radio"/> No	Healthcare	<input checked="" type="radio"/> Yes <input type="radio"/> No	MOU	
Local Government Agency	CPS, Tumor Board	<input checked="" type="radio"/> Yes <input type="radio"/> No	Healthcare	<input checked="" type="radio"/> Yes <input type="radio"/> No	BAA/MOU for Data Exchange	
Research Entity	UCSF/NCIRE/NIH/DOD	<input checked="" type="radio"/> Yes <input type="radio"/> No	Research	<input checked="" type="radio"/> Yes <input type="radio"/> No	Internal	
<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:	Austin Automation Center					
(FY 2012) PIA: Secondary Use						
Will PII data be included with any secondary use request?	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input checked="" type="checkbox"/> Mental Health	<input checked="" type="checkbox"/> HIV	<input checked="" type="checkbox"/> Drug/Alcohol Counseling		
Check all that apply		<input checked="" type="checkbox"/> Sickle Cell	<input type="checkbox"/> Other (Explain on Tab 8)	<input checked="" 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 B) <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 B)					
Has the data provided been verified as complete?					
<input checked="" type="checkbox"/> Veteran Verified <input checked="" 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
Answer: RCS-10-1 (Destroy 6 years, 3 months after the creation date of the purchase order or 6 years, 3 months after the last entry in f				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: RCS-10-1 (To adhere to the retention and disposition requirements for VHA Central Office and field facilities Federal records)					
What are the procedures for eliminating data at the end of the retention period?					
Answer: San Francisco VAMC MCM 137-19 (Procedures for Document Destruction) - documents will be placed in designated shred bins throughout the facility for proper disposal or may be shredded with approved office shredders, etc. which will be destroyed on-site twice a week.					
Where are these procedures documented?					
Answer: San Francisco VAMC MCM 137-19 (Procedures for Document Destruction)					
How are data retention procedures enforced?					
Answer: San Francisco VAMC MCM 00-51 (Records and Information Management Policy) - Service chiefs are responsible for designating a Records Liaison and ensuring service staff are aware of and abide by the policy/retention schedule for their service/records; Records Manager will maintain the master file plan inventory and conduct internal reviews to assist services and other offices with maintaining records according to policy and report to the Service Chief and/or facility Leadership as needed when a service is not in compliance with the retention period.					
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 B)					
(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 B) <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 checked="" type="checkbox"/> Lightning Strike	<input checked="" type="checkbox"/> Terrorist
<input type="checkbox"/> Blizzard	<input checked="" type="checkbox"/> Flooding	<input checked="" type="checkbox"/> Malicious Code	<input checked="" 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 checked="" type="checkbox"/> Hail	<input checked="" type="checkbox"/> Personnel Unavailable	<input checked="" type="checkbox"/> Tsunami
<input checked="" type="checkbox"/> Component Failure	<input checked="" type="checkbox"/> HAZMAT Release/Spill	<input checked="" type="checkbox"/> Power Failure	<input checked="" type="checkbox"/> User Negligence
<input checked="" type="checkbox"/> Dam Failure	<input checked="" type="checkbox"/> Human Health Emergency	<input checked="" type="checkbox"/> Sabotage	<input checked="" type="checkbox"/> User Sabotage
<input checked="" type="checkbox"/> Dust/Debris	<input checked="" 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 checked="" type="checkbox"/> Indoor Humidity	<input checked="" type="checkbox"/> System Penetration	<input checked="" type="checkbox"/> Water Damage
<input type="checkbox"/> Extreme Heat	<input checked="" type="checkbox"/> Landslide	<input checked="" type="checkbox"/> System Tampering	<input checked="" 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.

Answer:

privacy, medical, proprietary, financial, investigative, contractor sensitive, security management, etc.							
--	--	--	--	--	--	--	--

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)

<input checked="" 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 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.

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)

<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.

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)

<input checked="" 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 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?		
Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial		Automated Medical Information Exchange II (AIME II)
Agent Orange	BCMA Contingency Machines	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)
	Courseware Delivery System (CDS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)	Dental Records Manager	
	Education Training Website	Compensation & Pension 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
	Electronic Payroll Deduction (EPD)	Electronic Performance Support System (EPSS)
CONDO PUD Builder	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	
INS - BIRLS	Inventory Management System (IMS)	Modern Awards Process Development (MAP-D)
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		Purchase Order Management System (POMS)
	Loan Guaranty Training Website	Reinstatement Entitlement Program for Survivors (REAPS)
MES		Reserve Educational Assistance Program CH 1607
Mobilization	Mental Health Assistant	RightFax
Montgomery GI Bill	National Silent Monitoring (NSM)	Service Member Records Tracking System
MUSE	Powerscribe Dictation 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)	
Script Pro	Spinal Bifida Program Ch 18	VA Reserve Educational Assistance Program
SHARE	State Benefits Reference System	Veterans Assistance Discharge System (VADS)
Sidexis	State of Case/Supplemental (SOC/SSOC)	Veterans Exam Request Info System (VERIS)
	Telecare Record Manager	Veterans Insurance Claims Tracking and Response System (VICTARS)
Synquest		Veterans Service Representative (VSR) Advisor
VBA Training Academy	VBA Enterprise Messaging System	Vocational Rehabilitation & Employment (VR&E) CH 31
Veterans Canteen Web		
VETSNET Housekeeping	Web Electronic Lender Identification	Web Automated Folder Processing System (WAFFS)
		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 2012) PIA: Minor Applications A-M

Which of these are sub-components of your system?			
1184 Web	Clinx	Electronic signature	Imaging
AAP	Clinical Case Registries	Embedded Fragment Registry	Incentive Awards
ACCU Care	Clinical Data Repository/Health Data Repository	ENCORE 2	Incident Reporting
ACCU Check	Clinical Info Resource Network	ENDSOFT	Income Verification Match
ACCU Mwd	Clinical Monitoring System	Engineering	Incomplete Records Trading
Adobe Acrobat	Clinical Notes Templates	Enrollment Application System	Inpatient Medications
ADP Planning (PlanMan)	Clinical Procedures	Enterprise Technology Server & VNA Enterprise Technology Services	Intake/Output
ADT	Clinical Reminders	ePROMISE	Integrated Billing
Adverse Reaction Tracking	Clipboard	Equipment/ Turn-in Request	Integrated Patient Funds
Agent Cashier	Combat Veteran Outreach	Event Capture	Interim Management Support
Air Fortress	Committee on Waiver and Compromises	Event Driven Reporting	Inventory Management System
ASISTS	Consult/ Request Tracking	Extensible Editor	Kernel
Authorization/ Subscription	Controlled Correspondence	External Peer Review	Kids
Auto Instrument	Controlled Substances	ETECAP	KOWA
Auto Replenishment/ Ward Stock	CPRE	Fee Based Claims System	Lab Service
AUTOCAD	CPRS	Fee Based	Laboratory Electronic Data Interchange
Automated Access Request	CPT/ HCPCS Codes	Financial and Accounting System (FAS)	Letterman
Automated Info Collection Sys	Credentis Tracking	Financial Management System (FMS)	Lexicon Utility
Automated Lab Instruments	Credit Card Authentication	Functional Independence	Library
Automated Med Info Exchange	Data Innovations	Gen. Med. Rec. - IO	List Manager
Automated Sales Reporting	DELIVEREX	Gen. Med. Rec. - Vitals	Lynn Duresse Alarm
AutoMed	Denial	Gen. Med. Rec. - Generator	Mallman
Bad Code Med Admin	DICATION/Power Scribe	GENEX	MCCR National Database
Barcode Medication Administration Contingency Plan (BCU)	Dietetics	Generic Code Sheet	Meadows (MDVS)
BCMA Contingency Workstations	Discharge Summary	GeneSys	Medicine
BDN 301	Drug Grouper	Get Well Networks	Mental Health
Beneficiary Travel	BPM Plus	GEMD	MHTP
Big Fix	Drug Accountability	GREC	MICOM
CA Verified Components - DSSI	D91T	Health Data and Informatics	Microsoft Exchange E-mail System
Capacity Management - RUM	DSS Extracts	Health Level Seven	Military/Vet Eye Injury Registry
Capacity Management Tools	DSS Quadrant	Health Summary	Minimal Patient Dataset
CAARI	DSS Whiteboard (AVID)	Health Summary Contingency	Missing Patient Reg. (Original) A4EL
Cardiff Teleform	Education Tracking	HINQ	Mumps Audio/FX
Cardiology Systems (stand alone servers from the network)	EEO Complaint Tracking	Hospital Based Home Care	MyHealthEye
Care Management	EKS System	ICB	
CareTracker	Electronic Card System (ECD)	ICR - Immunology Case Registry	
CHECKPOINT	Electronic Payroll Deduction (EPD)	JFCAP	
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: VISTA 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
NDL	PGIS OR	Sentillion	VeteransCmteem Web
Network Health Exchange	Police & Security	Shift Change Handoff Tool	Veterans Information Solution
NOAH/INK	Problem List	Shoner id	VHA/UNAP1
NOIS	Progress Notes	Social Work	VHA/UNFPC1
Nursing Service	Prosthetics	Stellent	VHS & PA Tracking System
Occurrence Screen	Purchase Order Management System	Stentor	Visit Tracking
Omicell	Pyis	Surgey	VISTA RAD
Oncology	Q-Matic	Survey generator	VISTA RO
Onviford (VADG)	QMSI Prescription Processing	Telecare Record Manager	VISALINK
Opfill	Quality Assurance Integration	Temp Trak	VISALINK Security
Order Entry/ Results Reporting	Quality Improvement Checkdsk	Text Integration Utilities	Visual Impairment Services Team ANRV
Outpatient Pharmacy	QUASER	Tracker Database	Vtria BusinessWare
P2000 ROBOT	Rad/dlog/ Nuclear Medicine	Toolkit	VYXS
PACS database	RAFT	Topcon	Voluntary Timekeeping
Patch Module	RAIS	TracMaster	Voluntary Timekeeping National
Patient Data Exchange	Record Tracking	Trading Continuing Education	WEB HING
Patient Feedback	Registration	Traumatic Brain Injury	Whiteboard
Patient Representative	Release of Information - DSI	Umwinder	Women's Health
PCC Patient Care Encounter	Remote Order/ Entry System	Utility Management Rollup	Workload and Overtime
Personal Computer Generated Letters	Rac Broker	Utilization Review	
Pharmacy Benefits Management	Run Time Library	VA Conference Room Registration	
	SAGE	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 2012) PIA: Final Signatures		*Green Highlight = Must Answer Question	
Facility Name:	San Francisco VA Medical Center		
Title:	Name:	Phone:	Email:
Privacy Officer:	Elaine Tran	415-221-4810 x2135	elaine.tran@va.gov
Information Security Officer:	Dennis Lawton	x2141	dennis.lawton@va.gov
System Owner/Delegate:	Judith Ringler	415-221-4810 x6968	judith.ringler@va.gov
Chief Information Officer:	Judith Ringler	415-221-4810 x6968	judith.ringler@va.gov
Other Titles:		0	00
Date of Report:	04/2012		
OMB Unique Project Identifier	029-00-02-00-01-1120-00		
Project Name	Region1/VHA/VISN21/ San Francisco VAMC/ Local Area Network (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. 			