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.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program.
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.

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

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

Roles and Responsibilities:

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.

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.

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

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.

Privacy Impact Assessment Uploaded into SMART

All PIA Validation Letters should be mailto Christina.Pettit@va.gov to receive full credit for submission.

Various Privacy Data Websites:

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

Schedule FY 2012 : http://www.privacy.va.gov/PRIVACY/Privacy_Impact_Assessment.asp

(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 21> Northern California HCS> PBX		
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)"	VANCHCS uses the Private Branch eXchange (PBX) as a General Support System, supporting mission-critical and other systems necessary to conduct day-to-day operations within the Department of Veterans. PBX is a stand-alone system that does not store nor use Protected Health Information (PHI) or Personally Identifiable Information (PII)		
Facility or Program Office Name:	Veterans Affairs Northern California Health Care System (VANCHCS)		
Title:	Name:	Phone:	Email:
Privacy Officer:	Shannon Caston	707-437-1823	shannon.caston@va.gov
Information Security Officer:	Sharon Harris	916-843-9048	sharon.harris@va.gov
System Owner/Delegate:	Ron Walker	925-372-2197	ron.walker3@va.gov
Chief Information Officer:	Ron Walker	925-372-2197	ron.walker3@va.gov
Information Owner:	Brian J. O'Neill, (SES EQV)	916-843-9058	Brian.O'Neill@va.gov
Other Titles:	Terence Gant	707-437-1848	terence.gant@va.gov
Person Completing Document:	Alfredo S. Carpio Jr.	650-269-0052	alfredo.carpio@va.gov
Other Titles:			
Date of Last Full Approved PIA by VACO Privacy Services: (MM/YYYY)			01/2009
What specific legal authorities authorize this program or system:	Title 5 U.S. Code		
What is the expected number of individuals that will have their PII stored in this system:			0
Identify what stage the System / Application / Program is at:			Operations/Maintenance
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.			Approximately more than 9 years
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			
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 Secuirty System under 40 U.S.C. 11103, a PIA is not required for this system		
identifier?	○ Yes ◉ No		
6. What is the System of Records Notice (SORN) for this system?			
7. Has this SORN been reviewed or updated within the last three years?			
Date of Report (MM/YYYY):			20-Jan-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 2012) PIA: System of Records

*Green Highlight = Must Answer Question

1. Is a SORN (System of Records Notice) Required? ○ Yes ◉ No ○ Not Sure
2. Is there a SORN already in place? ○ Yes ◉ No

***If Yes, select all of the appropriate SORN number(s):
***If Not Sure, contine 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) :

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)

- ☐ 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
- ☐ Other (Explain on Tab 8)

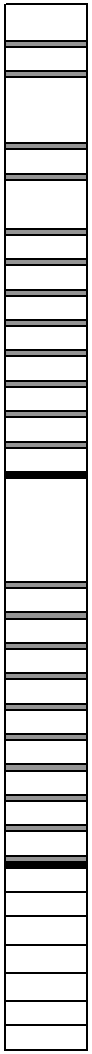
4. Based on Question 3, is a SORN required? ○ Yes ◉ No NO
***If Yes, has the process begun to obtain/acquire a SORN ○ Yes ◉ No Not Applicable
Location where the specific applicable System of Records Notice may be accessed:

(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)	N/A			
Family Relation (spouse, children, parents, grandparents, etc)	N/A			
Service Information	N/A			
Medical Information	N/A			
Criminal Record Information	N/A			
Guardian Information	ALL			
Education Information	N/A			
Benefit Information	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		○ Mandatory ◉ Voluntary	
Family Relation (spouse, children, parents, grandparents, etc)	○ Yes ◉ No		○ Mandatory ◉ Voluntary	
Service Information	○ Yes ◉ No		○ Mandatory ◉ Voluntary	
Medical Information	○ Yes ◉ No		○ Mandatory ◉ Voluntary	
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 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		○ Yes ◉ No		○ Yes ◉ No		
Other Veteran Organization		○ Yes ◉ No		○ Yes ◉ No		
Other Federal Government Agency		○ Yes ◉ No		○ Yes ◉ No		
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 2012) PIA: Access to Records						
Does the system gather information from another system?	○ Yes ◉ No					
Please enter the name of the system:						
(FY 2012) 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 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?

○ Yes (Explain on Tab 8) ◉ No

Is the data collected to only what is necessary to provide requested service?

◉ Yes ○ No (Explain on Tab 8)

Has the data provided been verified as complete?

☐ Veteran Verified ☐ Received From Database ☐ Verification Unknown

(FY 2012) PIA: Retention & Disposal

What is the data retention period?

Answer:

RCS 10-1 link for VHA: www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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:

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

Answer:

Where are these procedures documented?

Answer:

How are data retention procedures enforced?

Answer:

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

◉ Yes ○ 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?

○ Yes (Explain on Tab 8) ◉ 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.	◉ 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

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

Answer: Locally implemented along with VISN and Region controls are implemented to mitigate risks.

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

(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	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 Performace 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 Trancking 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 2012) PIA: Minor Applications A-M

Which of these are sub-components of your system?

1184 Web	**Citrix**	**Electronic Signature**	**Imaging**
A4P	**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 Med	**Clinical Monitoring System**	**Engineering**	**Incomplete Records Tracking**
Adobe Acrobat	**Clinical Notes Templates**	**Enrollment Application System**	**Inpatient Medications**
ADP Planning (PlanMan)	**Clinical Procedures**	**Enterprise Terminology Server & VHA Enterprise Terminology Services**	**Intake/ Output**
ADT	**Clinical Reminders**	**ePROMISE**	**Integrated Billing**
Adverse Reaction Tracking	**Clippership**	**Equipment/ Turn-in Request**	**Integrated Patient Funds**
Agent Cashier	**Combat Veteran Outreach**	**Event Capture**	**Interim Mangement Support**
Air Fortress	**Committee on Waiver and Compromises**	**Event Driven Reporting**	**Inventory Management System**
ASISTS	**Consult/ Request Tracking**	**Extensible Editor**	**Kernal**
Authorization/ Subscription	**Controlled Correspondence**	**External Peer Review**	**Kids**
Auto Instrument	**Controlled Substances**	**EYECAP**	**KOWA**
Auto Replenishment/ Ward Stock	**CP&E**	**Fee Based Claims System**	**Lab Service**
AUTOCAD	**CPRS**	**Fee Basis**	**Laboratory Electronic Data Interchange**
Automated Access Request	**CPT/ HCPCS Codes**	**Financial and Accounting System (FAS)**	**Letterman**
Automated Info Collection Sys	**Credentials 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. - I/O**	**List Manager**
Automated Sales Reporting	**DELIVEREX**	**Gen. Med. Rec. - Vitals**	**Lynx Duress Alarm**
AutoMed	**Dental**	**Gen. Med.Rec. - Generator**	**Mailman**
Bad Code Med Admin	**DICTATION-Power Scribe**	**GENDEX**	**MCCR National Database**
Barcode Medication Administration Contingency Plan (BCU)	**Dietetics**	**Generic Code Sheet**	**Meadows (MDWS)**
BCMA Contingency Workstations	**Discharge Summary**	**Genesys**	**Medicine**
BDN 301	**DRG Grouper**	**Get Well Networks**	**Mental Health**
Beneficiary Travel	**DRM Plus**	**GMED**	**MHTP**
Big Fix	**Drug Accountability**	**GRECC**	**MICOM**
CA Vertified Components - DSSI	**DSIT**	**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 Quadramed**	**Health Summary**	**Minimal Patient Dataset**
CAPRI	**EDS Whiteboard (AVJED)**	**Health Summary Contingency**	**Missing Patient Reg (Original) A4EL**
Cardiff Teleform	**Education Tracking**	**HINQ**	**Mumps AudioFAX**
Cardiology Systems (stand alone servers from the network)	**EEO Complaint Tracking**	**Hospital Based Home Care**	**MyHealthEVet**
Care Management	**EKG System**	**ICB**	
CareTracker	**Electronic Card System (ECD)**	**ICR - Immunology Case Registry**	
CHECKPOINT	**Electronic Payroll Deduction (EPD)**	**IFCAP**	

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**
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 Mangement	**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 2012) PIA: Final Signatures *Green Highlight = Must Answer Question

Facility Name:	Veterans Affairs Northern California Health Care System (VANCHCS)		
Title:	Name:	Phone:	Email:
Privacy Officer:	Shannon Caston	707-437-1823	shannon.caston@va.gov
Shannon T. Caston	Digitally signed by Shannon T. Caston DN: c=US, o=U.S. Government, ou=Department of Veterans Affairs, ou=Internal Staff, 0.9.2342.19200300.100.1.1=shannon.caston@va.gov, cn=Shannon T. Caston Date: 2012.02.02 14:12:23 -08'00'		
Information Security Officer:	Sharon Harris	916-843-9048	sharon.harris@va.gov
Sharon L. Harris	Digitally signed by Sharon L. Harris DN: c=US, o=U.S. Government, ou=Department of Veterans Affairs, ou=Internal Staff, 0.9.2342.19200300.100.1.1=sharon.harris@va.gov, cn=Sharon L. Harris Date: 2012.02.02 16:19:23 -08'00'		
System Owner/Delegate:	Ron Walker	925-372-2197	ron.walker3@va.gov
Ronald L. Walker	Digitally signed by Ronald L. Walker DN: c=US, o=U.S. Government, ou=Department of Veterans Affairs, ou=Internal Staff, 0.9.2342.19200300.100.1.1=ron.walker3@va.gov, cn=Ronald L. Walker Date: 2012.02.03 08:30:07 -08'00'		
Chief Information Officer:	Ron Walker	925-372-2197	ron.walker3@va.gov
Ronald L. Walker	Digitally signed by Ronald L. Walker DN: c=US, o=U.S. Government, ou=Department of Veterans Affairs, ou=Internal Staff, 0.9.2342.19200300.100.1.1=ron.walker3@va.gov, cn=Ronald L. Walker Date: 2012.02.03 08:30:25 -08'00'		
Other Titles:	Terence Gant	707-437-1848	terence.gant@va.gov
William T. Gant	Digitally signed by William T. Gant DN: c=US, o=U.S. Government, ou=Department of Veterans Affairs, ou=Internal Staff, 0.9.2342.19200300.100.1.1=terence.gant@va.gov, cn=William T. Gant Date: 2012.02.02 09:40:57 -08'00'		
Date of Report:	20-Jan-12		
OMB Unique Project Identifier	029-00-02-00-01-1120-00		
Project Name	REGION 1> VHA> VISN 21> Northern California HCS> PBX		

The Signature Process:

- Complete the PIA form.
- Name the PIA Excel FORM [“FY12-Region # - Facility Name - Facility # -Date(mmddyyyy).xls”]
- 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
- If no errors, convert form into PDF with Nuance PDF Professional.
- Name the PIA PDF form [“FY12-Region #-Facility Name- Facility # -Date(mmddyyyy).xls”]
- Obtain digital signatures on the “Final Signatures tab”
- Submit signed PIA PDF form to the SMART Database.