

Welcome to the PIA for FY 2011!

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.

PIA Website: http://vawww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

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

- a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA 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. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

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.

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

Privacy Impact Assessments should be uploaded into C&A section of SMART.

All PIA Validation Letters should be emailed to christina.pettit@va.gov to received full credit for submission.

(FY 2011) PIA: System Identification

Program or System Name: REGION 1> VHA> VISN21> PALO ALTO HCS> VistA
 OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-01-11-01-1180-00

REGION 1> VHA> VISN21> PALO ALTO HCS> VistA located at Sacramento RDPC including the system boundary, the FIPS 199 Impact Level of HIGH, and the FIPS 200 security controls as tailored specifically for this system. Each Veterans Affairs (VA) medical center uses VistA Legacy (formerly DHCP, Decentralized Hospital Computer Program), an integrated hospital information system. DHCP was an M-based internally developed portfolio and VistA Legacy encompasses DHCP and a variety of other clinical and administrative applications, some on single-use platforms. VistA Legacy is currently running on two core platforms, Microsoft Windows 2000 (W2K)/Cache and Virtual Memory System (VMS)/Cache. VistA Legacy is structured so that it can be customized in certain specialized areas and most local medical centers have taken advantage of this flexibility. Applications within VistA Legacy support a multitude of areas including medical imaging, supply management, decision support, medical research, and education. VHA began deploying DHCP in 1982 with a core set of applications. Today, VistA Legacy is one of the most comprehensive integrated health information systems in the United States. Since episode-of-care workload reporting was an initial motivation for corporate databases, most of VHA's corporate systems collect their information from VistA Legacy. Recent enhancements have clearly shifted the focus from workload to enabling the integration of clinical information from various disciplines, forming the basis for an automated and distributed health information system.

Description of System/ Application/ Program:

Facility Name: Palo Alto HCS

Title:	Name:	Phone:	Email:
Privacy Officer:	Ana Marie Vitente	650-493-5000 x64616	anamarie.vitente@va.gov
Information Security Officer:	Alfredo Carpio Jr.	650-269-0052	alfredo.carpio@va.gov
System Owner/ Chief Information Officer:	Doug Wirthgen	650-849-0402	doug.wirthgen@va.gov
Chief, VistA Management Section	Minerva Sims	650.493.5000 x66074	minerva.sims@va.gov
Information Security Officer:	Freddie Cobb	650.493.5000 x63844	freddie.cobb@va.gov
Person Completing Document:	Freddie Cobb	650.493.5000 x63844	freddie.cobb@va.gov

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY) 03/2009
 Date Approval To Operate Expires: 08/2011

What specific legal authorities authorize this program or system: 38 USC 7301(a)

What is the expected number of individuals that will have their PII stored in this system: Over 85,000 enrollees

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. 01/1994

Is there an authorized change control process which documents any changes to existing applications or systems?

Yes

If No, please explain:

Has a PIA been completed within the last three years? Yes

Date of Report (MM/YYYY): 01/2011

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

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

If there is no Personally Identifiable Information on your system , please complete TAB 7 & TAB 12. (See Comment for Definition of PII)

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15. Yes

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

- | | |
|---|--|
| 1. All System of Record Identifier(s) (number): | 02VA135, 07VA138, 14VA135, 23VA163, 24VA19, 29VA11, 32VA00, 33VA113, 34VA12, 57VA10C2, 64VA15 , 65VA122, 77VA10Q, 79VA19, 89VA19, 98VA104A, 99VA131, 100VA10NS10, 113VA112, 114VA16, 121 VA19, 130VA19, 150VA19, 155VA16, and 04VA115. |
|---|--|

Applicants for employment under Title 38 (USCVA), Department of Medicine and Surgery Engineering Employee Management Information Records-VA, Individuals Serving on a Fee Basis or Without Compensation, Non-VA Fee basis Records-VA, Patient Medical Records-VA, Physician, Dentist, and Supervisory Nurse Professional Standards Board Action File-VA, Veteran, Employee, and Citizen Health Care Facility Investigation Records-VA, National Prosthetics Patient Database-VA, Veteran, Patient, Employee and Volunteer Research and Development Project Records-VA, Voluntary Service Records-VA, Readjustment Counseling Service (RCS) Vet Center Program-VA, Community Placement Program-VA, Health Care Provider Credentialing and Privileging Records-VA, Veterans Health Information System and Technology Architecture (VISTA), Health Eligibility Records-VA, Disaster Emergency Medical Personnel System- VA (DEMPS),Automated Safety Incident Tracking System-VA

2. Name of the System of Records:

3. Location where the specific applicable System of Records Notice may be accessed (include the URL):

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

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)? Yes

Does the System of Records Notice require modification or updating? Yes

(Please Select Yes/No)

- | | |
|--|-----|
| Is PII collected by paper methods? | Yes |
| Is PII collected by verbal methods? | Yes |
| Is PII collected by automated methods? | Yes |
| Is a Privacy notice provided? | Yes |
| Proximity and Timing: Is the privacy notice provided at the time of data collection? | Yes |
| Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used? | Yes |
| Authority: Does the privacy notice specify the effects of providing information on a voluntary basis? | Yes |
| Disclosures: Does the privacy notice specify routine use(s) that may be made of the information? | Yes |

(FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Paper	Benefits (Billing Purposes), Healthcare Management (Treatment), Healthcare Operations, and Research	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	Paper	Benefits (Billing Purposes), Healthcare Management (Treatment), Healthcare Operations, and Research	Written	Written
Service Information	Electronic/File Transfer	Benefits (Billing Purposes), Healthcare Management (Treatment), Healthcare Operations, and Research	Written	Written
Medical Information	Electronic/File Transfer	Name, full SSN, address, date of birth, phone number, service connection, etc. The data is used for treatment, payment and health care purposes.	Written	Written
Criminal Record Information	Electronic/File Transfer	This information is only available in the HRMS department VA Police Service and used for personnel, investigatory, and contracting purposes.	Written	Written
Guardian Information	Paper	Name, address, phone number, e-mail address, etc. The data is used for treatment, payment and health care purposes.	Written	Written
Education Information	Paper	Patient and employment records. Employee training records. The data is used for treatment, payment and health care purposes.	Written	Written
Benefit Information	Paper	Patient and employment records. The data is used for treatment, payment and health care purposes.	Written	Written
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Voluntary	Full name, social security number, date of birth, address, and phone number. The data is used for direct patient care treatment, insurance claims, billing payment and facility health care operations purposes.
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	Service connection, other medical insurance, e-mail address, fax number, etc. The data is used for treatment, payment and health care purposes.
Service Information	Yes	Veteran	Voluntary	Name, full SSN, address, date of birth, phone number, service connection, etc Used for patient Benefits and service administrative employment records.
Medical Information	Yes	Veteran	Mandatory	Name, full SSN, address, date of birth, phone number, service connection, etc. The data is used for treatment, payment and health care purposes.
Criminal Record Information	Yes	Veteran	Mandatory	This information is only available in the HRMS department VA Police Service and used for personnel, investigatory, and contracting purposes.
Guardian Information	Yes	Veteran	Voluntary	Name, address, phone number, e-mail address, etc. The data is used for treatment, payment and health care purposes.
Education Information	Yes	Veteran	Voluntary	Patient and employment records. Employee training records. The data is used for treatment, payment and health care purposes.
Benefit Information	Yes	Veteran	Mandatory	Patient and employment records. The data is used for treatment, payment and health care purposes.
Other (Explain)				
Other (Explain)				
Other (Explain)				

(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VA Palo Alto Health Care System	Yes	Valid users with active VistA codes and identified with the need-to-know.	Both PII & PHI	ROI authorization is not required for employees of VAPAHCS to access and use of information to perform healthcare duties.
Other Veteran Organization	VSO	Yes	Valid users with active VistA codes and identified with the need-to-know.	Both PII & PHI	Read-only access allowed. ROI to VSO with valid representation and authorization from Veteran.
Other Federal Government Agency	DOD, DOJ, OIG, and HHS	Yes	Valid users with active VistA codes and identified with the need-to-know.	Both PII & PHI	Through MOUs, ROI procedures, standing letters, etc.
State Government Agency	Cancer Registry, Tumor Board, APS, CPS, and DMV	No	Mandatory reporting to State authorities.	Both PII & PHI	Through standing letters.
Local Government Agency	Cancer Registry, Tumor Board, APS, CPS, and DMV	No	Mandatory reporting to State authorities.	Both PII & PHI	Through standing letters.
Research Entity	Various pharmaceutical sponsors and other VA Research centers	No	Research information specific to the study	Both PII & PHI	Data Transfer/Usage Agreements, Business Associate Agreements, and/or Offsite Data Storage Waivers.
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system?	Yes
Please enter the name of the system:	Stentor for radiology images, Clients HL7, XRAD - radiology (local), PICIS - ICU units (VISN), Polytrauma - VHAPALPACS (Presidential Mandate), RDI/MDS - Nursing (National), CP Metafusion - Will replace GI (local), Research servers, Health Care Operations Reports servers, VBA and OPM
Per responses in Tab 4, does the system gather information from an individual?	Yes
If information is gathered from an individual, is the information provided:	<input checked="" type="checkbox"/> Through a Written Request <input checked="" type="checkbox"/> Submitted in Person <input checked="" type="checkbox"/> Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	Yes

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?	No
if yes, please check all that apply:	<input type="checkbox"/> Drug/Alcohol Counseling <input type="checkbox"/> Mental Health <input type="checkbox"/> HIV <input type="checkbox"/> Research <input type="checkbox"/> Sickle Cell <input type="checkbox"/> Other (Please Explain)
Describe process for authorizing access to this data.	
Answer:	

(FY 2011) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: Responses are based only on questions asked.

How is data checked for completeness?

Answer: Data is reviewed by staff and compared records on VISTA system.

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

Answer: Clinical Data is not removed. Administrative data is updated with each episode of care.

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

Answer: Data is verified from source of information.

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: Clinical information is retained in accordance with VA Records Control Schedule 10-1. Demographic information is updated as applications for care are submitted and retained in accordance with VA RCS 10-1.

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

Answer: For Healthcare

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

Answer: Electronic final version of patient medical record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA RCS 10-1, Item XLIII 2.b (Page 190) and in the local policy based on 6500 handbook

Where are these procedures documented?

Answer: VA Handbook 6500; RCS 10-1

How are data retention procedures enforced?

Answer: RCS 10-1, page 8

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

Yes

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2011) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?

No

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 2011) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	Yes
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..	Yes
Is security monitoring conducted on at <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Is security testing conducted on at <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Are performance evaluations conducted on at <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
If 'No' to any of the 3 questions above, please describe why: Answer:	
Is adequate physical security in place to protect against unauthorized access? If 'No' please describe why: Answer:	Yes

Explain how the project meets IT security requirements and procedures required by federal law.
 Answer: i. At the Department level the CIO's Office of Cyber Security (OCS) is responsible for the establishment of directives, policies, and procedures which are consistent with the provisions of Federal Information Security Management Act (FISMA) as well as guidance issued by the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and other requirements that Vista-Legacy is and has been subject to. In addition, OCS administers and manages Department-wide security solutions such as anti-virus protection, authentication, vulnerability scanning and penetration testing, intrusion detection systems, and incident response (800-61). At the Vista-Legacy project level- the Project Manager ensures that CIO-provided security directives are integrated into the project's security plan & implemented by VA & contractor staff throughout the project. Funding needs are dependent on IT security requirements identified in the system develop life cycle (800-64) (i.e., risk assessments (800-30), certification and accreditation (800-37 and 800-53), as well as identified security weaknesses that must be corrected.

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

- | | | |
|---|--|--|
| <input checked="" type="checkbox"/> Air Conditioning Failure | <input checked="" type="checkbox"/> Data Disclosure | <input checked="" type="checkbox"/> Hardware Failure |
| <input checked="" type="checkbox"/> Chemical/Biological Contamination | <input checked="" type="checkbox"/> Data Integrity Loss | <input checked="" type="checkbox"/> Identity Theft |
| <input type="checkbox"/> Blackmail | <input checked="" type="checkbox"/> Denial of Service Attacks | <input checked="" type="checkbox"/> Malicious Code |
| <input type="checkbox"/> Bomb Threats | <input type="checkbox"/> Earthquakes | <input checked="" type="checkbox"/> Power Loss |
| <input checked="" type="checkbox"/> Burglary/Break In/Robbery | <input type="checkbox"/> Eavesdropping/Interception | <input checked="" type="checkbox"/> Sabotage/Terrorism |
| <input checked="" type="checkbox"/> Cold/Frost/Snow | <input type="checkbox"/> Errors (Configuration and Data Entry) | <input checked="" type="checkbox"/> Storms/Hurricanes |
| <input type="checkbox"/> Communications Loss | <input checked="" type="checkbox"/> Fire (False Alarm, Major, and Minor) | <input type="checkbox"/> Substance Abuse |
| <input checked="" type="checkbox"/> Computer Intrusion | <input checked="" type="checkbox"/> Flooding/Water Damage | <input checked="" type="checkbox"/> Theft of Assets |
| <input checked="" type="checkbox"/> Computer Misuse | <input checked="" type="checkbox"/> Fraud/Embezzlement | <input checked="" type="checkbox"/> Theft of Data |
| <input type="checkbox"/> Data Destruction | | <input checked="" type="checkbox"/> Vandalism/Rioting |

Answer: (Other Risks)

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"/> Contingency Planning | <input checked="" type="checkbox"/> Personnel Security |
| <input checked="" type="checkbox"/> Audit and Accountability | <input checked="" type="checkbox"/> Identification and Authentication | <input checked="" type="checkbox"/> Physical and Environmental Protection |
| <input checked="" type="checkbox"/> Awareness and Training | <input checked="" type="checkbox"/> Incident Response | <input checked="" type="checkbox"/> Risk Management |
| <input checked="" type="checkbox"/> Certification and Accreditation Security Assessments | | |
| <input checked="" type="checkbox"/> Configuration Management | <input checked="" type="checkbox"/> Media Protection | |

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer: i. Vista-Legacy is a steady state project and is governed by existing policies and procedures.

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.

Please add additional controls:

(FY 2011) 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 2011) 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)
Appraisal System	Benefits Delivery Network (BDN)	Automated Medical Information System (AMIS)290
ASSISTS	Centralized Property Tracking System	Automated Standardized Performance Elements Nationwide (ASPEN)
Awards	Common Security User Manager (CSUM)	Centralized Accounts Receivable System (CARS)
Awards	Compensation and Pension (C&P)	Committee on Waivers and Compromises (COWC)
Baker System	Control of Veterans Records (COVERS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)	Control of Veterans Records (COVERS)	Compensation & Pension Training Website
BDN Payment History	Control of Veterans Records (COVERS)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
BIRLS	Courseware Delivery System (CDS)	Distribution of Operational Resources (DOOR)
C&P Payment System	Dental Records Manager	Educational Assistance for Members of the Selected Reserve Program CH 1606
C&P Training Website	Education Training Website	Electronic Performance Support System (EPSS)
CONDO PUD Builder	Electronic Appraisal System	Enterprise Wireless Messaging System (Blackberry)
Corporate Database	Electronic Card System (ECS)	Financial Management Information System (FMI)
Data Warehouse	Electronic Payroll Deduction (EPD)	Hearing Officer Letters and Reports System (HOLAR)
EndoSoft	Eligibility Verification Report (EVR)	Inquiry Routing Information System (IRIS)
FOCAS	Fiduciary Beneficiary System (FBS)	Modern Awards Process Development (MAP-D)
Inforce	Fiduciary STAR Case Review	Personnel and Accounting Integrated Data and Fee Basis (PAID)
INS - BIRLS	Financial and Accounting System (FAS)	Personal Computer Generated Letters (PCGL)
Insurance Online	Insurance Unclaimed Liabilities	Personnel Information Exchange System (PIES)
Insurance Self Service	Inventory Management System (IMS)	Personnel Information Exchange System (PIES)
LGY Home Loans	LGY Centralized Fax System	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing	Loan Service and Claims	Purchase Order Management System (POMS)
Mobilization	Loan Guaranty Training Website	Reinstatement Entitlement Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Assistant	Service Member Records Tracking System
Omniceil	National Silent Monitoring (NSM)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Powerscribe Dictation System	Systematic Technical Accuracy Review (STAR)
RAI/MDS	Rating Board Automation 2000 (RBA2000)	Training and Performance Support System (TPSS)
Right Now Web	Rating Board Automation 2000 (RBA2000)	VA Online Certification of Enrollment (VA-ONCE)
SAHSHA	Rating Board Automation 2000 (RBA2000)	VA Reserve Educational Assistance Program
Script Pro	Records Locator System	Veterans Appeals Control and Locator System (VACOLS)
SHARE	Review of Quality (ROQ)	Veterans Assistance Discharge System (VADS)
SHARE	Search Participant Profile (SPP)	Veterans Exam Request Info System (VERIS)
SHARE	Spinal Bifida Program Ch 18	Veterans Service Representative (VSR) Advisor
Sidexis	State Benefits Reference System	Vocational Rehabilitation & Employment (VR&E) CH 31
Synquest	State of Case/Supplemental (SOC/SSOC)	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
VBA Data Warehouse	Telecare Record Manager	Web Automated Folder Processing System (WAFPS)
VBA Training Academy	VBA Enterprise Messaging System	Web Automated Reference Material System (WARMS)
Veterans Canteen Web	Veterans On-Line Applications (VONAPP)	Web Automated Verification of Enrollment
VIC	Veterans Service Network (VETSNET)	Web-Enabled Approval Management System (WEAMS)
VR&E Training Website	Web Electronic Lender Identification	Web Service Medical Records (WebSMR)
Web LGY		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 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

ASISTS	Beneficiary Travel	Accounts Receivable	Adverse Reaction Tracking
Bed Control	Care Management	ADP Planning (PlanMan)	Authorization/ Subscription
CAPRI	Care Tracker	Bad Code Med Admin	Auto Replenishment/ Ward Stock
CMOP	Clinical Reminders	Clinical Case Registries	Automated Info Collection Sys
Dental	CPT/ HCPCS Codes	Clinical Procedures	Automated Lab Instruments
Dietetics	DRG Grouper	Consult/ Request Tracking	Automated Med Info Exchange
Fee Basis	DSS Extracts	Controlled Substances	Capacity Management - RUM
GRECC	Education Tracking	Credentials Tracking	Capacity Management Tools
HINQ	Engineering	Discharge Summary	Clinical Info Resource Network
IFCAP	Event Capture	Drug Accountability	Clinical Monitoring System
Imaging	Extensible Editor	EEO Complaint Tracking	Enrollment Application System
Kernal	Health Summary	Electronic Signature	Equipment/ Turn-in Request
Kids	Incident Reporting	Event Driven Reporting	Gen. Med.Rec. - Generator
X Lab Service	Intake/ Output	External Peer Review	Health Data and Informatics
Letterman	X Integrated Billing	Functional Independence	ICR - Immunology Case Registry
Library	Lexicon Utility	Gen. Med. Rec. - I/O	Income Verification Match
Mailman	List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
X Medicine	Mental Health	Generic Code Sheet	Interim Mangement Support
MICOM	X MyHealthEVet	Health Level Seven	Master Patient Index VistA
NDBI	National Drug File	Hospital Based Home Care	Missing Patient Reg (Original) A4EL
NOIS	Nursing Service	X Inpatient Medications	Order Entry/ Results Reporting
Oncology	Occurrence Screen	Integrated Patient Funds	PCE Patient Care Encounter
PAID	Patch Module	MCCR National Database	Pharmacy Benefits Mangement
Prosthetics	Patient Feedback	Minimal Patient Dataset	Pharmacy Data Management
QUASER	Police & Security	National Laboratory Test	Pharmacy National Database
RPC Broker	Problem List	Network Health Exchange	Pharmacy Prescription Practice
SAGG	Progress Notes	X Outpatient Pharmacy	Quality Assurance Integration
Scheduling	Record Tracking	Patient Data Exchange	Quality Improvement Checklist
Social Work	Registration	Patient Representative	X Radiology/ Nuclear Medicine
X Surgery	Run Time Library	PCE Patient/ HIS Subset	Release of Information - DSSI
Toolkit	Survey Generator	Security Suite Utility Pack	Remote Order/ Entry System
Unwinder	Utilization Review	Shift Change Handoff Tool	Utility Management Rollup
VA Fileman	Visit Tracking	Spinal Cord Dysfunction	CA Verified Components - DSSI
VBECS	VistALink Security	Text Integration Utilities	X Vendor - Document Storage Sys
VDEF	Women's Health	VHS & RA Tracking System	Visual Impairment Service Team ANRV
VistALink		Voluntary Timekeeping	Voluntary Timekeeping National

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

Name	HealtheVet Web Services Client (HWSC)		
Description	HWSC is a communications tool, that can be used by other VistA applications to make requests from VistA to an external web service (e.g., Health Data Repository/HDR), and get a response/result back. On its own, HWSC does not initiate any communications. All data sent/received is specific to the VistA application using HWSC, and is not initiated by HWSC itself.		
Comments	The only data HWSC collects, from IRM and other VistA applications, are the names/locations of external web servers/services that IRM and other VistA applications have configured		
Is PII collected by this minor application?		NO	
Does this minor application store PII?		NO	
If yes, where?			
Who has access to this data?	The non-PII data stored by HWSC is accessible only by holders of the "@" FileMan security key, which is typically restricted to IRM only.		

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 2011) PIA: Minor Applications

Which of these are sub-components of your system?

1184	Web	ENDSOFT	RAFT	
		Enterprise Terminology Server &	RALS	
A4P		VHA Enterprise Terminology Services		
	Administrative Data Repository (ADR)	ePROMISE	Remedy Application	
	ADT	EYECAP	SAN	
	Agent Cashier	Financial and Accounting System (FAS)	Scanning Exam and Evaluation System	
	Air Fortress	Financial Management System (FMS)	Sentillion	
X	Auto Instrument	Genesys	Stellant	
	Automated Access Request	Health Summary Contingency	X	Stentor
	BDN 301	ICB	Tracking Continuing Education	
	Bed Board Management System	KOWA	Traumatic Brain Injury	
	Cardiff Teleform	Lynx Duress Alarm	VA Conference Room Registration	
	Cardiology Systems (stand alone servers from the network)		MHTP	VAMedSafe
	CHECKPOINT	Microsoft Active Directory	VBA Data Warehouse	
	Clinical Data Repository/Health Data Repository		Microsoft Exchange E-mail System	VHAHUNAPP1
	Combat Veteran Outreach	Military/Vet Eye Injury Registry	VHAHUNFPC1	
	Committee on Waiver and Compromises	Mumps AudioFAX	VISTA RAD	
	CP&E	NOAHLINK	Whiteboard	
	Crystal Reports Enterprise X	Omnicell		
	Data Innovations	Onvicord (VLOG)		
X	DELIVEREX	Optifill		
	DICTATION-Power Scribe	X	P2000 ROBOT	
	DRM Plus	PACS database		
	DSIT	Personal Computer Generated Letters		
X	DSS Quadramed X	PICIS OR		
	EDS Whiteboard (AVJED)	PIV Systems		
X	EKG System (MUSE)	Q-Matic		
	Embedded Fragment Registry	QMSI Prescription Processing		

(FY 2011) PIA: Final Signatures

Facility Name: REGION 1> VHA> VISN21> PALO ALTO HCS> VistA

Title:	Name:	Phone:	Email:
--------	-------	--------	--------

Privacy Officer:	Ana Marie Vitente	650-493-5000 x64616	anamarie.vitente@va.gov
------------------	-------------------	------------------------	-------------------------

Ana Marie S. Vitente



Digitally signed by Ana Marie S. Vitente
DN: cn=US, o=U.S. Government, ou=Department of Veterans Affairs,
ou=Internal Staff, 0.9.2342.19200300.100.1.1=anamarie.vitente@va.gov,
c=Ana Marie S. Vitente
Date: 2011.01.19 14:58:21 -0800'

Information Security Officer:	Alfredo Carpio Jr.	650-269-0052	alfredo.carpio@va.gov
-------------------------------	--------------------	--------------	-----------------------

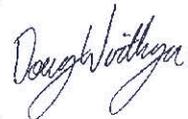
Alfredo S. Carpio Jr.



Digitally signed by Alfredo S. Carpio
DN: cn=US, o=U.S. Government, ou=Department of Veterans Affairs,
ou=Internal Staff, 0.9.2342.19200300.100.1.1=alfredo.carpio@va.gov,
cn=Alfredo S. Carpio
Date: 2011.01.13 09:44:39 -08'00'

System Owner/ Chief Information Officer:	Doug Wirthgen	650-849-0402	doug.wirthgen@va.gov
--	---------------	--------------	----------------------

Doug Wirthgen



Digitally signed by Doug Wirthgen
DN: cn=Doug Wirthgen, o=OI&T, ou=640 - Palo Alto, CA, email=Doug.Wirthgen@va.gov, c=US
Date: 2011.01.12 16:27:10 -08'00'

Chief, VistA Management Section	Minerva Sims	650.493.5000 x66074	minerva.sims@va.gov
---------------------------------	--------------	------------------------	---------------------

MINERVA SIMS



Digitally signed by MINERVA SIMS
DN: cn=Department of Veterans Affairs, ou=Dept. of Veterans Affairs, Internal Staff, ou=www.verisign.com/repository/CPS In corp. by Ref., LIA B.LTD c396, cn=MINERVA SIMS, email=minerva.sims@va.gov
Date: 2011.01.13 09:32:52 -08'00'

Information Security Officer:	Freddie Cobb	650.493.5000 x63844	freddie.cobb@va.gov
-------------------------------	--------------	------------------------	---------------------

FREDDIE R COBB



Digitally signed by FREDDIE R COBB
DN: o=Department of Veterans Affairs, ou=Dept. of Veterans Affairs, Internal Staff, ou=www.verisign.com/repository/CPS In corp. by Ref., LIA B.LTD c396, cn=FREDDIE R COBB, email=freddie.cobb@va.gov
Date: 2011.01.13 11:23:44 -08'00'

Date of Report: 1/0/00
 OMB Unique Project Identifier: 029-00-02-00-01-1120-00
 Project Name: REGION 1> VHA> VISN21> PALO ALTO HCS> VistA



Digitally signed by Alfredo S. Carpio
DN: cn=US, o=U.S. Government, ou=Department of Veterans Affairs,
ou=Internal Staff, 0.9.2342.19200300.100.1.1=alfredo.carpio@va.gov,
cn=Alfredo S. Carpio
Date: 2011.01.18 09:19:50 -08'00'