

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> VISN 22> Long Beach Healthcare System
 OMB Unique System / Application / Program Identifier (AKA: UPID #):

Description of System/ Application/ Program: The VistA-Legacy system is the software platform and hardware that VHA health care facilities operate their software applications. The VistA-Legacy system is a client-server system. It links the facilities and equipment associated with clinical operations and the information systems. VistA-Legacy is a client-server system. It links the facilities and equipment associated with clinical operations and the information systems. VistA-Legacy system supported IT services across the VA Health Care Networks (VISNs) that managed 155 medical centers, 135 treatment programs, 135 nursing homes, 207 readjustment centers, 135 national cemeteries. VistA-Legacy provides critical data for VA health care dependants. Using the computer, the VA health care personnel manage health care data needs. The VistA-Legacy system operates in VA health care homes and domiciliary. The VistA-Legacy system is in the

Facility Name:	VA Long Beach Healthcare System	
Title:	Name:	Phone:
Privacy Officer:	Jenny Fan	(562) 826-8000 x4521
Information Security Officer:	Jeremy R. Chongco	(562) 826-8000 x4647
System Owner/ Chief Information Officer:	Rodney A. Sagmit	(562) 826-5789
Information Owner:	Isabel Duff	(562) 826-5400
Other Titles:		
Person Completing Document:	Jeremy R. Chongco	(562) 826-8000 x4647
Other Titles:		
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)		
Date Approval To Operate Expires:		

What specific legal authorities authorize this program or system:
 What is the expected number of individuals that will have their PII stored in this system:
 Identify what stage the System / Application / Program is at:
 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.

System - Legacy
029-00-01-11-01-1180-00

hardware infrastructure (associated with clinical operations) on which the operations and support for E-Government initiatives. It includes the computer employees (approximately 3000 FTE) necessary to operate the system. The system is a large computer network to over 100 applications and databases. In 2006, the system was transferred to VistA-Legacy, a VA organization which had a network of 23 Veterans Integrated Service Centers (VISCs) and over 881 community based outpatient clinics, 46 residential rehabilitation centers, 57 veteran benefits regional offices, and 125 community-based health centers that supports the delivery of healthcare to veterans and their families. The system provider can access VistA-Legacy applications and meet a wide range of needs in medical centers, ambulatory and community-based clinics, nursing homes, and in the mature phase of the capital investment lifecycle.

Email:

jia.fan2@va.gov jeremy.chongco@va.gov rodney.sagmit@va.gov isabel.duff2@va.gov
jeremy.chongco@va.gov

10/2010
08/2011

Title 38, United States Code, section 7301(a).
460,000 - 500,000
Operations/Maintenance

20+ years

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

If No, please explain:

Has a PIA been completed within the last three years?

Date of Report (MM/YYYY):

Please check the appropriate boxes and continue to the next TAB and complete the remaining question

- 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

Yes

Yes

01/2011

ns on this form.

employees, contractors, or others performing work for
of name, unique identifier, symbol, or

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):

79VA19

2. Name of the System of Records:

Veterans Health Information Systems and Technology Architecture (VistA)

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

<http://vawww.vhaco.va.gov/privacy/SystemofRecords.htm>

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?

No

(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)	Verbal	This patient information falls into two classes: administrative and clinical. Clinical information is used to diagnose, prescribe treatment and follow clinically the patient through his/her health care encounters. Administrative data is used to identify the veteran (SSN), correspond to/from (name and address), and determine eligibility (patient administrative info + SSA and IRS data).	Written	Written
Family Relation (spouse, parents, etc)	Verbal	Next-of-kin information and emergency contact information, such as name and telephone number, is collected from the veteran to use to contact other individuals in case of an emergency. In addition insurance and employment information is available on the veteran for use in billing for care.	Verbally	Written
Service Information	Paper	This information is collected to assess eligibility for VA healthcare benefits, type of healthcare needed.	Written	Written

VistA-Legacy applications and meet a wide range of health care data needs. The VistA-Legacy system operates in medical centers, ambulatory and community-based clinics, nursing homes and domiciliary, and thus collects a wide range of personal medical information for clinical diagnosis, treatment, patient evaluation, and patient care. Common types of personal medical information would include lab test results, prescriptions, allergies, medical diagnoses, vital signs, etc. The information is used to treat and care for the veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of the veteran.

Medical Information	Verbal		Verbally	Written
Criminal Record Information		N/A		
Guardian Information	Verbal	This information is used in the notification process and as required for medical decisions.	Written	Written
Education Information	Paper	This information is voluntary.	Verbally	Verbally
Benefit Information	Paper	This information is used to determine what benefits the veterans have or have used.	Verbally	Verbally
Other (Explain) - Rehabilitation Information	Paper	Treatment notes, progress notes, clinical assessments, clinical diagnosis information is collected. Used in follow-up treatment and as part of the medical history.	Verbally	Written

Other (Explain) - Next-of-kin information and emergency contact information	Verbal	Next-of-kin information and emergency contact information, such as name and telephone number, is collected from the veteran to use to contact other individuals in case of an emergency. In addition insurance and employment information is available on the veteran for use in billing for care.	Verbally	Written
---	--------	--	----------	---------

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	Mandatory	
Family Relation (spouse, parents, etc.)	Yes	Veteran	Voluntary	
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Medical Information	Yes	Veteran	Voluntary	
Criminal Record Information	No			
Guardian Information	Yes	Veteran	Voluntary	
Education Information	Yes	Other (Explain)	Voluntary	Provided by VA Employee
Benefit Information	Yes	Veteran	Voluntary	
Other (Explain) - Rehabilitation Information	Yes	VA Files / Databases (Identify file)	Voluntary	
Other (Explain) - Next of-kin	Yes	Veteran	Voluntary	

(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	Yes	configuration mgmt	N/A	
Other Veteran Organization	Department of Defense	Yes	clinical data	N/A	
Other Federal Government Agency	N/A				
State Government Agency	N/A				
Local Government Agency	N/A				
Research Entity	N/A				
Other Project / System	N/A				
Other Project / System	N/A				
Other Project / System	N/A				

(FY 2011) PIA: Access to Records

Does the system gather information from another system? No

Please enter the name of the system:

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:

Through a Written Request
 Submitted in Person
 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?

Drug/Alcohol Counseling
 Mental Health
 HIV
 Research
 Sickle Cell
 Other (Please Explain)

if yes, please check all that apply:

Describe process for authorizing access to this data.
 Answer: Patient consent is required prior to authorizing access to this data.

(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: Data is collected electronically based on the automation of VA Forms and clinical procedures.

How is data checked for completeness?

Answer: Data is reviewed by staff and compared to paper forms. Various audits such as medical record audit, compliance audits in MCCR, etc.

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

Answer: Clinical data is not removed. Clinical and admin data is updated with each application for care.

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

Answer: New data is compared with printed form or via patient verification.

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 (IAW) VA Records Control Schedule 10-1. Demographic information is updated as applications for care are submitted and retained IAW VA RCS 10-1. Data is retained for 75 years.

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

Answer: It is needed for daily business operations and patient care.

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

Where are these procedures documented?

Answer: VA Handbook 6300; RCS 10-1

How are data retention procedures enforced?

Answer: VA Records Control Schedule 10-1 (page 8): Records Management Responsibilities The Health Information Resources Service (HIRS) is

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 least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Are performance evaluations conducted on at least 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? Yes

If 'No' please describe why:

Answer:

Explain how the project meets IT security requirements and procedures required by federal law.

Answer: At the Department level the CIO's Office of Cyber & Information Security (OCIS) is responsible for the establishment of directives, policies, &

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 checked="" type="checkbox"/> Blackmail | <input checked="" type="checkbox"/> Denial of Service Attacks | <input checked="" type="checkbox"/> Malicious Code |
| <input checked="" type="checkbox"/> Bomb Threats | <input checked="" type="checkbox"/> Earthquakes | <input checked="" type="checkbox"/> Power Loss |
| <input checked="" type="checkbox"/> Burglary/Break In/Robbery | <input checked="" type="checkbox"/> Eavesdropping/Interception | <input checked="" type="checkbox"/> Sabotage/Terrorism |
| <input checked="" type="checkbox"/> Cold/Frost/Snow | <input checked="" type="checkbox"/> Errors (Configuration and Data Entry) | <input checked="" type="checkbox"/> Storms/Hurricanes |
| <input checked="" type="checkbox"/> Communications Loss | <input checked="" type="checkbox"/> Fire (False Alarm, Major, and Minor) | <input checked="" 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 checked="" 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: Look at the entire system with emphasis on the security measures taken for control, audit, consent, configuration mgmt, maintenance, and

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

VBA Data Warehouse
VBA Training Academy
Veterans Canteen Web
VIC
VR&E Training Website
Web LGY

Telecare Record Manager
VBA Enterprise Messaging System
Veterans On-Line Applications (VONAPP)
Veterans Service Network (VETSNET)
Web Electronic Lender Identification

Web Automated Folder Processing System (WAFPS)
Web Automated Reference Material System (WARMS)
Web Automated Verification of Enrollment
Web-Enabled Approval Management System (WEAMS)
Web Service Medical Records (WebSMR)
Work Study Management System (WSMS)

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

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

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

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

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

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

Name	Health Management System
Description	Pull patient visits and prescriptions to connect to external insurance info, sent back to upload
Comments	
Is PII collected by this minor application?	y
Does this minor application store PII?	yes
If yes, where?	at vendor site and on Vista
Who has access to this data?	Vendor HMS staff and insurance verifiers

Name	Omnicell
Description	inpatient medication orders information and stocking
Comments	
Is PII collected by this minor application?	y
Does this minor application store PII?	yes
If yes, where?	omicell server
Who has access to this data?	Omnicell us

Name	ADDS
Description	interface between ADDS machine and outpatient pharmacy orders
Comments	
Is PII collected by this minor application?	y
Does this minor application store PII?	y
If yes, where?	on ADDS machine and Vista
Who has access to this data?	Outpatient pharmacy staff and CBOC medical staff

Name DHCPFax
Description faxing material orders to vendors
Comments
Is PII collected by this minor application?N
Does this minor application store PII?No
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	X	
Administrative Data Repository (ADR)	ePROMISE	X	Remedy Application
X ADT	EYECAP		SAN
X Agent Cashier	Financial and Accounting System (FAS)		Scanning Exam and Evaluation System
X Air Fortress	Financial Management System (FMS)	X	Sentillion
X Auto Instrument	Genesys		Stellant
Automated Access Request	X Health Summary Contingency		Stentor
BDN 301	X ICB		Tracking Continuing Education
X Bed Board Management System	KOWA		Traumatic Brain Injury
Cardiff Teleform	Lynx Duress Alarm		VA Conference Room Registration
X Cardiology Systems (stand alone servers from the network)	MHTP		VAMedSafe
CHECKPOINTX	Microsoft Active Directory		VBA Data Warehouse
X Clinical Data Repository/Health Data Repository	X Microsoft Exchange E-mail System		VHAHUNAPP1
Combat Veteran Outreach	Military/Vet Eye Injury Registry		VHAHUNFPC1
Committee on Waiver and CompromisesX	Mumps AudioFAX	X	VISTA RAD
CP&E X	NOAHLINK		Whiteboard
Crystal Reports Enterprise	X Omnicell		
Data Innovations	Onvicord (VLOG)		
DELIVEREX	Optifill		
DICTATION-Power Scribe	P2000 ROBOT		
X DRM Plus	X PACS database		
X DSIT	Personal Computer Generated Letters		
X DSS Quadramed	PICIS OR		
EDS Whiteboard (AVJED)	X PIV Systems		

X EKG System
Embedded Fragment Registry

Q-Matic
QMSI Prescription Processing

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	Dawning
Description	connects lab instruments with Vista
Comments	
Is PII collected by this minor application?N	
Does this minor application store PII?N	
If yes, where?	
Who has access to this data?	

(FY 2011) PIA: Final Signatures

Facility Name: Region 1> VHA> VISN 22> Long Beach Healthcare System - Legacy

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

Privacy Officer:	Jenny Fan	(562) 826-8000 x4521	jia.fan2@va.gov
------------------	-----------	-------------------------	-----------------

Digital Signature Block

Information Security Officer:	Jeremy R. Chongco	(562) 826-8000 x4647	jeremy.chongco@va.gov
-------------------------------	-------------------	-------------------------	-----------------------

Digital Signature Block

System Owner/ Chief Information Officer:	Rodney A. Sagmit	(562) 826-5789	rodney.sagmit@va.gov
--	------------------	----------------	----------------------

Digital Signature Block

Information Owner:

Digital Signature Block

Other Titles:	0	0	0
---------------	---	---	---

Digital Signature Block

Date of Report:	2/9/11
OMB Unique Project Identifier	029-00-01-11-01-1180-00

Project Name

Region 1> VHA> VISN 22> Long
Beach Healthcare System - Legacy