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://vaww.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 indentify 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 San Diego VAMC Vista-VMS		
OMB Unique System / Application / Program Identifier	(AKA: UPID #):	029-00-01-11-01-1180-00	

Description of System/ Application/ Program: The VistA-Legacy system is the software platform and hardware infrastructure (associated with clinical operations) on which the VHA health care facilities operate their software applications and support for E-Government initiatives. It includes the computer equipment associated with clinical operations and the employees (approximately 2500 FTE) necessary to operate the system. VistA-Legacy is a client-server system. It links the facility computer network to over 100 applications and databases. In 2006, the VistA-Legacy system supported IT services across the VA organization which had a network of 21 Veterans Integrated Service Networks (VISNs) that managed 155 medical centers, over 881 community based outpatient clinics, 46 residential rehabilitation treatment programs, 135 nursing homes, 207 readjustment counseling centers, 57 veteran benefits regional offices, and 125 national cemeteries. VistA-Legacy provides critical data that supports the delivery of healthcare to veterans and their dependants. Using the computer, the VA health care provider can access 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. The VistA-Legacy system is in the mature phase of the capital investment lifecycle.

Facility Name: San Diego VAMC

Title:	Name:	Phone:	Email:
Privacy Officer:	Mike DeShazer	858-552-8585, ext. 3941	Mike.Deshazer@va.gov
Information Security Officer:	Jesse Christmas	858-642-6200	Jesse.Christmas@va.gov
System Owner/ Chief Information Officer:	Duc D. Nguyen	858-642-3399	Duc.D.Nguyen@va.gov
Information Owner:	Duc D. Nguyen	858-642-3399	Duc.D.Nguyen@va.gov
Other Titles: Associate Chief, ITS	Ruey Keller	858-642-6420	Ruey.Keller@va.gov
Person Completing Document:	Kathy DeVierno, ISO	858-552-8585, ext. 1021	Kathleen.DeVierno@va.gov
Other Titles: Information Security Officer	Jeannie Pham	858-552-8586, ext 1559	Jeannie.Pham@va.gov
Date of Last PIA Approved by VACO Privacy Services:			08/2008
Date Approval To Operate Expires:			08/2011

What specific legal authorities authorize this program or system: Title 38, United States Code, section 7301 (a).

What is the expected number of individuals that will have their PII stored in this system:	50,000 to 100,000
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.	26 years
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 2 & 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):	79VA19
2. Name of the System of Records:	VistA-VA
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	http://vaww.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)	ALL	Benefits, Healthcare, Research	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	Verbal	Benefits, Healthcare, Research	Written	Written
Service Information	ALL	Benefits, Healthcare, Research	Written	Written
Medical Information	ALL	Benefits, Healthcare, Research	Written	Written
Criminal Record Information	Paper & Electronic	Healthcare	Written	Written
Guardian Information	Paper	Benefits, Healthcare, Research	Written	Written
Education Information	Paper & Electronic	Healthcare	Written	Written
Benefit Information	ALL	Healthcare & Benefits	Written	Verbal & 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)	No	Veteran	Mandatory	Data is stored at the Regional Data Center - Denver/San Diego

Family Relation (spouse, children, parents, grandparents, etc)	No	Veteran	Mandatory	Data is stored at the Regional Data Center - Denver/San Diego
Service Information	No	Veteran	Mandatory	Data is stored at the Regional Data Center - Denver/San Diego
Medical Information	No	Veteran	Mandatory	Data is stored at the Regional Data Center - Denver/San Diego
Criminal Record Information	No	Veteran	Voluntary	Data is stored at the Regional Data Center - Denver/San Diego
Guardian Information	No	Veteran	Mandatory	Data is stored at the Regional Data Center - Denver/San Diego
Education Information	No	Veteran	Voluntary	Data is stored at the Regional Data Center - Denver/San Diego
Benefit Information	No	VA Files / Databases (Identify file)	Mandatory	Data is stored at the Regional Data Center - Denver/San Diego VA FILES - HINQ
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	National VistA Support team	Yes	Dial into the system to resolve issues for a limited ammount of time	Both PII & PHI	VA Directive 6500
Other Veteran Organization	VBA	Yes	Compensation & Pension exams	Both PII & PHI	Information is shared through CAPRI and AMIE.
Other Federal Government Agency		No			
State Government Agency	State of California	No	As required by law information is shared with state agencies. A standing order is required to be in place before the information is shared.	Both PII & PHI	Covered by a standing letter with the government agency - Department of Motor Vehicles (report recurrent periods of loss of consciousness, physical or mental condition that may make a patient an unsafe driver.) Keep unsafe drivers off the roads State Cancer registry (report cancer patients seen at medical center on a monthly basis) The registry tracks Cancer in the state of California.

Local Government Agencies		No	As required by law information is shared with local/county agencies. A standing order is required to be in place before the information is shared.	Both PII & PHI	County Department Heath & Human Service - Department of Children and Families (report child abuse). We have a responsibility to insure the safety of a child. Local legal requirement mandates the release of information and a standing letter would be in effect. County Medical Examiner.
Research Entity	Varies	No	Part of the research protocol	Both PII & PHI	This varies from protocol to protocol. This release would either be consented by the patient or there would be a Data Use Agreement (DUA) in place.
Other Project / System Other Project / System Other Project / System	Social Secuirty Administration	No	release of medical records for processing claims with the Social Security Administration.	Both PII & PHI	VHA Directive 2010-009, Release of Information to Social Security Administration (SSA)

(FY 2011) PIA: Access to Records

Does the system gather information from another system? Yes

Please enter the name of the system: Health Eligibility Center (HEC) and VHA's Master Patient Index File

Per responses in Tab 4, does the system gather information from an individual?

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? Yes

if yes, please check all that apply:

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

Describe process for authorizing access to this data.

Answer: The veteran will consent to the use of this data as part of the Research Protocol.

(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 collected is set by the required fields in the VistA menu. Information is collected via the phone, web, paper-based forms, and in person to process applications for healthcare and is limited to what is needed to complete the registration process and to provide services to our veterans.

How is data checked for completeness?

Answer: Required data elements are driven by Vista software applications whereas the exclusion of essential information will not allow VA Staff to continue with the entry process. Upon exiting several Vista software applications if any data elements are missing a notification message is generated to the user and other VA staff of the missing data elements. Vista audit reports reveal missing data elements essential to the registration process, time & leave entry, patient documentation, etc. that are reviewed by VA staff. Compliance and Business Integrity monitors are in place to assure accuracy of data entry of various Vista software applications.

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

Answer: There are automatic reminders in place to ask veterans for update information when they come in for appointments. Staff is required to update various data elements in Vista during each patient encounter which occurs via the phone, the web, or in person.

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

Answer: Required data elements are driven by Vista software applications whereas the exclusion of essential information will not allow VA Staff to continue with the entry process. Upon exiting several Vista software applications if any data elements are missing a notification message is generated to the user and other VA staff of the missing data elements. Vista audit reports reveal missing data elements essential to the registration process, time & leave entry, patient documentation, etc. that are reviewed by VA staff. Compliance and Business Integrity monitors are in place to assure accuracy of data entry of various Vista software applications.

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

Answer: HINQS are also used to check the validity of the data supplied by the veteran. Veterans also have the opportunity to review the data that is in their medical record and ask for corrections to the record via the amendment process.

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: Information is retained according to the VA Records Control Schedule (RCS-10) for future treatment of the patients, for research purposes, legal issues and to investigate cause/effect of agents that were used during combat, i.e, Agent Orange to determine to the long term effect on the veteran population. Electronic Final Version of Patient Medical Record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records Control Schedule (RCS-10) 10-1, Item XLIII, 2.b. (Page 190). At the present time, VistA Imaging retains all images. VHA is performing a study to explore whether some images can be eliminated on an earlier schedule. Researchers are responsible for destroying research records as per the RCS which is undergoing revision.
Paper records shipped to the national archive will be destroyed by the agency after the 75 year retention requirement is met.

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

Answer: The retention is set by the Record Control Schedule (RCS-10) and varies according the documents. Information needs to be retained to document VA business for future reference.

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 Records Control Schedule (RCS-10) 10-1, Item XLIII, 2.b. (Page 190). At the present time, VistA Imaging retains all images. VHA is performing a study to explore whether some images can be eliminated on an earlier schedule. Researchers are responsible for destroying research records as per the RCS which is undergoing revision.
Paper records shipped to the national archive will be destroyed by the agency after the 75 year retention requirement is met.

Where are these procedures documented?
Answer: VA Directive 6300.1, Record Management Procedures, Record Control Schedule (RCS-10), VA Directive 6371 and current VA standards on the disposal of sensitive information

How are data retention procedures enforced?
Answer: Field records officers are responsible for records management activities at this facility. In addition, ITOC will review record management procedures when they conduct audits.

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 Information and Technology (OI&T) is responsible for the establishment of directives, policies, &

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

- [x] Air Conditioning Failure
- [ ] Chemical/Biological Contamination
- [ ] Blackmail
- [ ] Bomb Threats
- [ ] Burglary/Break In/Robbery
- [ ] Cold/Frost/Snow
- [x] Data Disclosure
- [x] Data Integrity Loss
- [x] Denial of Service Attacks
- [ ] Earthquakes
- [ ] Eavesdropping/Interception
- [x] Hardware Failure
- [x] Identity Theft
- [x] Malicious Code
- [x] Power Loss
- [ ] Sabotage/Terrorism
- [x] Storms/Hurricanes

- [x] Communications Loss
- [x] Computer Intrusion
- [x] Computer Misuse
- [x] Data Destruction
- [x] Errors (Configuration and Data Entry)
- [x] Fire (False Alarm, Major, and Minor)
- [x] Flooding/Water Damage
- [x] Fraud/Embezzlement
- [ ] Substance Abuse
- [x] Theft of Assets
- [x] Theft of Data
- [ ] Vandalism/Rioting

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

- ☑ Access Control
- ☑ Audit and Accountability
- ☑ Awareness and Training
- ☑ Certification and Accreditation Security Assessments
- ☑ Configuration Management
- ☑ Contingency Planning
- ☑ Identification and Authentication
- ☑ Incident Response
- ☑ Media Protection
- ☑ Personnel Security
- ☑ Physical and Environmental Protection
- ☑ Risk Management

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: Areas to reconsider Collection of data; collection methods; controls to mitigate misuse.

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 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 Bed Control
X CAPRI
X CMOP
X Dental
X Dietetics
X Fee Basis
GRECC
X HINQ
X IFCAP
X Imaging
Kernal
X Kids
X Lab Service
Letterman
X Library
X Mailman
X Medicine
MICOM
X NDBI
X NOIS
X Oncology
X PAID
X Prosthetics
X QUASER
X RPC Broker
X SAGG
X Scheduling
X Social Work
X Surgery
X Toolkit
X Unwinder
X VA Fileman
X VBECS
X VDEF
X VistALink

X Beneficiary Travel
X Care Management
X Care Tracker
X Clinical Reminders
X CPT/ HCPCS Codes
X DRG Grouper
X DSS Extracts
Education Tracking
X Engineering
X Event Capture
Extensible Editor
X Health Summary
X Incident Reporting
Intake/ Output
X Integrated Billing
X Lexicon Utility
X List Manager
X Mental Health
X MyHealthEVet
X National Drug File
X Nursing Service
X Occurrence Screen
Patch Module
X Patient Feedback
X Police & Security
X Problem List
X Progress Notes
X Record Tracking
X Registration
X Run Time Library
X Survey Generator
X Utilization Review
X Visit Tracking
X VistALink Security
X Women's Health

X Accounts Receivable
ADP Planning (PlanMan)
X Bad Code Med Admin
X Clinical Case Registries
X Clinical Procedures
X Consult/ Request Tracking
X Controlled Substances
X Credentials Tracking
X Discharge Summary
X Drug Accountability
X EEO Complaint Tracking
X Electronic Signature
X Event Driven Reporting
X External Peer Review
X Functional Independence
X Gen. Med. Rec. - I/O
X Gen. Med. Rec. - Vitals
X Generic Code Sheet
X Health Level Seven
X Hospital Based Home Care
X Inpatient Medications
Integrated Patient Funds
X MCCR National Database
X Minimal Patient Dataset
X National Laboratory Test
X Network Health Exchange
X Outpatient Pharmacy
X Patient Data Exchange
X Patient Representative
PCE Patient/ HIS Subset
Security Suite Utility Pack
X Shift Change Handoff Tool
X Spinal Cord Dysfunction
X Text Integration Utilities
VHS & RA Tracking System
X Voluntary Timekeeping

X Adverse Reaction Tracking
X Authorization/ Subscription
X Auto Replenishment/ Ward Stock
X Automated Info Collection Sys
X Automated Lab Instruments
X Automated Med Info Exchange
X Capacity Management - RUM
Capacity Management Tools
X Clinical Info Resource Network
X Clinical Monitoring System
X Enrollment Application System
X Equipment/ Turn-in Request
X Gen. Med.Rec. - Generator
X Health Data and Informatics
X ICR - Immunology Case Registry
X Income Verification Match
X Incomplete Records Tracking
X Interim Mangement Support
X Master Patient Index VistA
X Missing Patient Reg (Original) A4EL
X Order Entry/ Results Reporting
X PCE Patient Care Encounter
X Pharmacy Benefits Mangement
X Pharmacy Data Management
X Pharmacy National Database
X Pharmacy Prescription Practice
X Quality Assurance Integration
X Quality Improvement Checklist
X Radiology/ Nuclear Medicine
X Release of Information - DSSI
X Remote Order/ Entry System
X Utility Management Rollup
X CA Vertified Components - DSSI
X Vendor - Document Storage Sys
X Visual Impairment Service Team ANRV
X 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	ACCU CARE
Description	Patient Assessment tool in Extended Care
Comments	
Is PII collected by this minor application?	YES
Does this minor application store PII?	YES
If yes, where?	Server that contains the information is stored in the IT Computer Room
Who has access to this data?	IT system Administrators and the clinical staff in Extended Care.

Name	VistA Read Only (VistA RO)
Description	Back-up of VistA information to be used when VistA is down.
Comments	
Is PII collected by this minor application?	YES
Does this minor application store PII?	YES
If yes, where?	Server in the ITS Computer Room
Who has access to this data?	IT system administrators and the clinical staff and medica center staff who

Name	Mumps Audio Care
Description	Device that connects to VistA to automatically call veterans to remind them of their appointments
Comments	
Is PII collected by this minor application?	YES
Does this minor application store PII?	YES
If yes, where?	Server in the ITS Computer Room
Who has access to this data?	IT Admins

(FY 2011) PIA: Minor Applications

Which of these are sub-components of your system?

1184 Web	ENDSOFT	RAFT
A4P	Enterprise Terminology Server & VHA Enterprise Terminology Services	RALS

(FY 2011) PIA: Final Signatures

Facility Name: Region 1 VHA VISN 22 San Diego VAMC Vista-VMS

Title:	Name:	Phone:	Email:
Privacy Officer:	Mike DeShazer	858-552-8585, ext. 3941	Mike.Deshazer@va.gov
Information Security Officer:	Jesse Christmas	858-642-6200	Jesse.Christmas@va.gov
System Owner/ Chief Information Officer:	Duc D. Nguyen	858-642-3399	Duc.D.Nguyen@va.gov
Information Owner:	Duc D. Nguyen	858-642-3399	Duc.D.Nguyen@va.gov
Other Titles: Associate Chief, ITS	Ruey Keller	858-642-6420	Ruey.Keller@va.gov

Date of Report:	1/19/11
OMB Unique Project Identifier	029-00-01-11-01-1180-00
Project Name	Region 1 VHA VISN 22 San Diego VAMC Vista-VMS

(FY 2011) PIA: Final Signatures

Facility Name: Region 1 VHA VISN 22 San Diego VAMC Vista-VMS

Title:	Name:	Phone:	Email:
Privacy Officer:	Mike DeShazer	858-552-8585, ext. 3941	Mike.Deshazer@va.gov
Information Security Officer:	Jesse Christmas	858-642-6200	Jesse.Christmas@va.gov
System Owner/ Chief Information Officer:	Duc D. Nguyen	858-642-3399	Duc.D.Nguyen@va.gov
Information Owner:	Duc D. Nguyen	858-642-3399	Duc.D.Nguyen@va.gov
Other Titles: Associate Chief, ITS	Ruey Keller	858-642-6420	Ruey.Keller@va.gov

Mike DeShazer MS/MHM/HCI CIPP/G/IT 1/20/11

Date of Report: 1/19/11

OMB Unique Project Identifier 029-00-01-11-01-1180-00

Project Name Region 1 VHA VISN 22 San Diego VAMC Vista-VMS