

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 2010) PIA: System Identification

Program or System Name:

Vista-Legacy

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 on which the VHA health care facilities operate their software applications and support for E-Government initiatives. In October 1996, Congress enacted the Veterans' Health Care Eligibility Reform Act of 1996, Public Law 104-262, which required VHA to implement a priority-based enrollment system. The Enrollment project includes functionality to process veterans' applications for enrollment, share veterans' eligibility and enrollment data with all VA health care facilities involved in the veterans' care, manage veterans' enrollment correspondence and telephone inquiries, and support national reporting and analysis of enrollment data. The Health Eligibility Center (HEC) Legacy system handles this functionality. Enrollment Operations and Maintenance supports the maintenance of the HEC Legacy system until it is replaced by Enrollment System Redesign (ESR) 3.0 in September 2008. There may be a several month overlap of the legacy and replacement systems until it is verified that ESR 3.0 is completely operational.

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: Health Eligibility Center

Title: Name:

Privacy Officer: Dee Tyner

Information Security Officer: Michael Francis

Chief Information Officer: Chuck Shrader

Person Completing Document: Michael Francis

Other Titles: Information Owner Tony Guagliardo

Other Titles:

Other Titles:

Date of Last PIA Approved by VACO Privacy Services:

(MM/YYYY) 08/2010

Date Approval To Operate Expires: 07/2011

What specific legal authorities authorize this program or system: Title 38 U.S.C. Section 1705 , and Public Law 104-262 38 U.S.C. Sections 1705, 1710, 1712, and 1722 along with Title 38 US code Section 7301(a).

What is the expected number of individuals that will have their PII stored in this system:

1,000,000 - 9,999,999

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.

01/1992

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 skip to TAB 12. (See Comment for Definition of PII)



Phone: Email:

404-828-5211	Dee.Tyner@va.gov
404-828-5319	Michael.Francis@va.gov
404-828-5200	Chuck.Shrader@va.gov
404-828-5319	Michael.Francis@va.gov
404-828-5300	Tony.Guagliardo@va.gov



(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): **89VA19 and 147VA16**
2. Name of the System of Records: **Income Verification Records and Healthcare Eligibility Records - VA**

3. Location where the specific applicable System of Records Notice may be accessed (include the URL): **http://vawww.vhaco.va.gov/privacy/Update_SOR/ListVHASORS.doc and <http://a257.g.akamaitech.net/7/257/2422/01jan20081800/edocket.access.gpo.gov/2008/pdf/E8-5956.pdf>**

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**

Is PII collected by paper methods? **Yes**

Is PII collected by verbal methods? **No**

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)	Electronic/File Transfer	establish and maintain applicants' records necessary to support the delivery of health care benefits; establish applicants' eligibility for VA health care benefits	Verbal & Written	Verbal & Written
Family Relation (spouse, children, parents, grandparents, etc)	Electronic/File Transfer	establish and maintain applicants' records necessary to support the delivery of health care benefits; establish applicants' eligibility for VA health care benefits	Verbal & Written	Verbal & Written
Service Information	Electronic/File Transfer	establish and maintain applicants' records necessary to support the delivery of health care benefits; establish applicants' eligibility for VA health care benefits	Verbal & Written	Verbal & Written
Medical Information	Electronic/File Transfer	establish and maintain applicants' records necessary to support the delivery of health care benefits; establish applicants' eligibility for VA health care benefits	Verbal & Written	Verbal & Written
Criminal Record Information	Electronic/File Transfer	establish and maintain applicants' records necessary to support the delivery of health care benefits; establish applicants' eligibility for VA health care benefits	Verbal & Written	Verbal & Written
Guardian Information	Electronic/File Transfer	establish and maintain applicants' records necessary to support the delivery of health care benefits; establish applicants' eligibility for VA health care benefits	Verbal & Automatic	Verbal & Written
Education Information	Electronic/File Transfer	establish and maintain applicants' records necessary to support the delivery of health care benefits; establish applicants' eligibility for VA health care benefits	Verbal & Written	Verbal & Written
Benefit Information	ALL	establish and maintain applicants' records necessary to support the delivery of health care benefits; establish applicants' eligibility for VA health care benefits	Verbal & 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)	Yes	VA Files / Databases (Identify file)	Voluntary	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Voluntary	
Service Information	Yes	VA Files / Databases (Identify file)	Voluntary	
Medical Information	No	VA Files / Databases (Identify file)	Voluntary	
Criminal Record Information	No	VA Files / Databases (Identify file)	Voluntary	
Guardian Information	No	VA Files / Databases (Identify file)	Voluntary	
Education Information	No	VA Files / Databases (Identify file)	Voluntary	
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	
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	VBA VHA	Yes	VBA data used for income verification to determine eligibility for benefits	PII	The Privacy Act of 1974 (Section 552a of Title 5 of the United States Code) and VA Handbook 6300.5 "Procedures for Establishing & Managing Privacy Act Systems Of Records"
Other Veteran Organization					
Other Federal Government Agency	IRS,SSA, DOD		SSN, Federal Tax Information	PII	The Privacy Act of 1974 (Section 552a of Title 5 of the United States Code) and VA Handbook 6300.5 "Procedures for Establishing & Managing Privacy Act Systems Of Records"
State Government Agency		No			
Local Government Agency		No			
Research Entity					
Other Project / System		No			
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: WebHinq, Share and VIS

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? No

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: N/A

(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: For the electronic VA Form 10-10EZ, certain fields are identified as required and veterans are not able to complete the form unless answered, although "none" or N/A is an acceptable response. Collected information is limited to information needed to make determinations on Veterans eligibility for VA Health Care Benefit veteran contact to include emergency contacts as well as next of kin. Information to determine billing criteria as well as those conditions for which there is no billing required.

How is data checked for completeness?

Answer: There are consistency checks within the system to determine if information complete. There is a possibility that some information will

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

Answer: Follow-up with individuals is conducted periodically at the VAMC to obtain updated information. For VBA related information, as updates are made, the information is PUSHED to the Enrollment system and that system shares the information with Vista.

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

Answer: Enrollment performs data integrity validation by comparing some data elements against the business requirements encapsulated within the business rule engine to ensure the accuracy and validity of the data elements.

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: Regardless of the record medium, all records are disposed of in accordance with the records retention standards approved by the Archivist of the United States, National Archives and Records Administration, and published in the VHA Records Control Schedule 10-1. Paper records are destroyed after they have been accurately scanned on optical disks. Optical disks or other electronic medium are deleted when all phases of the veteran's appeal rights have ended (ten years after the income year for which the means test verification was conducted).

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

Answer: The information is needed to maintain applicants' records necessary to support the delivery of health care benefits; establish applicants' eligibility for VA health care benefits; to operate an annual enrollment system; provide eligible veterans with an identification card; collect from health insurance providers for care of Nonservice-connected conditions; respond to inquiries related to VA health care benefits, enrollment and eligibility and compile management reports.

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

Answer: Regardless of the record medium, all records are disposed of in accordance with the records retention standards approved by the Archivist of the United States, National Archives and Records Administration, and published in the VHA Records Control Schedule 10-1. Depending on the record medium, records are destroyed by either shredding or degaussing.

Where are these procedures documented?

Answer: HEC Systems of Records: Health Eligibility Records-VA, 147VA16 and Income Verification Records - VA 89VA19.

How are data retention procedures enforced?

Answer: Retention procedures are enforced in accordance with VHA Handbook 1605.1, HEC Memorandum 742-35, "Privacy, Release of

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: The project follows the guidance published by the CIO's Office of Cyber and Information Security (OCIS), which establishes directives, policies,

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

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

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.

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.

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 **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.

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.

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 **moderate** if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments?

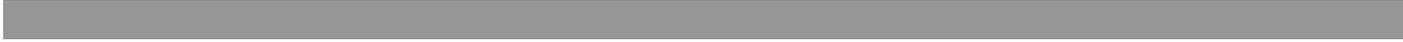
FALSE

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 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.

Please add additional controls:

20	TRUE	High
0	FALSE	Moderate
0	FALSE	Low



20	TRUE	High
0	FALSE	Moderate

0	FALSE	Low
---	-------	-----



20	TRUE	High
0	FALSE	Moderate
0	FALSE	Low
0 Total		

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

The VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow NIST SP800-53 moderate impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of this facility' common security controls. These issues are identified and described in the system security plans for the individual information systems.

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

(FY 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.

E P U V L t o s a v f o s a s t i n f p o H V L a n v n r o n I	
--	--

(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 Performace 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 Entitelment Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Asisstant	Service Member Records Tracking System
Omnicell	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
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?

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	X Capacity Management - RUM
GRECC	Education Tracking	Credentials Tracking	X Capacity Management Tools
X HINQ	Engineering	Discharge Summary	Clinical Info Resource Network
X IFCAP	Event Capture	Drug Accountability	Clinical Monitoring System
X Imaging	Extensible Editor	EEO Complaint Tracking	Enrollment Application System
X Kernal	Health Summary	X Electronic Signature	Equipment/ Turn-in Request
X Kids	Incident Reporting	Event Driven Reporting	Gen. Med.Rec. - Generator
Lab Service	Intake/ Output	External Peer Review	Health Data and Informatics
Letterman	Integrated Billing	Functional Independence	ICR - Immunology Case Registry
Library	Lexicon Utility	Gen. Med. Rec. - I/O	X Income Verification Match
X Mailman	List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine	Mental Health	Generic Code Sheet	Interim Mangement Support
MICOM	MyHealthEVet	X Health Level Seven	X Master Patient Index VistA
NDBI	National Drug File	Hospital Based Home Care	Missing Patient Reg (Original) A4EL
NOIS	Nursing Service	Inpatient Medications	Order Entry/ Results Reporting
Oncology	Occurrence Screen	Integrated Patient Funds	PCE Patient Care Encounter
PAID	X 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
X RPC Broker	Problem List	Network Health Exchange	Pharmacy Prescription Practice
X SAGG	Progress Notes	Outpatient Pharmacy	Quality Assurance Integration
Scheduling	Record Tracking	Patient Data Exchange	Quality Improvement Checklist
Social Work	Registration	Patient Representative	Radiology/ Nuclear Medicine
Surgery	Run Time Library	PCE Patient/ HIS Subset	Release of Information - DSSI
X Toolkit	Survey Generator	Security Suite Utility Pack	Remote Order/ Entry System
Unwinder	Utilization Review	Shift Change Handoff Tool	Utility Management Rollup
X VA Fileman	Visit Tracking	Spinal Cord Dysfunction	CA Verified Components - DSSI
VBECS	VistALink Security	Text Integration Utilities	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 wish to include.

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

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

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

(FY 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
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	Sentillion
Auto Instrument	Genesys	Stellant
Automated Access Request	Health Summary Contingency	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 Committee on Waiver and Compromises	Military/Vet Eye Injury Registry	VHAHUNFPC1
CP&E	Mumps AudioFAX	VISTA RAD
Crystal Reports Enterprise	NOAHLINK	Whiteboard
Data Innovations	Omnicell	
DELIVEREX	Onvicord (VLOG)	
	Optifill	

DICTATION-Power Scribe	P2000 ROBOT
DRM Plus	PACS database
DSIT	Personal Computer Generated Letters
DSS Quadramed	PICIS OR
EDS Whiteboard (AVJED)	PIV Systems
EKG System	Q-Matic
Embedded Fragment Registry	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. N/A

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

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

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

(FY 2011) PIA: Final Signatures

Facility Name: #REF!

Title:	Name:	Phone:	Email:
#REF!	Dee Tyner	404-828-5211	Dee.Tyner@va.gov
#REF!	Michael Francis	404-828-5319	Michael.Francis@va.gov
#REF!	Chuck Shrader	404-828-5200	Chuck.Shrader@va.gov
#REF!	Tony Guagliardo	404-828-5300	Tony.Guagliardo@va.gov
#REF!	Tyrone Wood	404-828-5200	Tyrone.Wood@va.gov

Date of Report: #REF!
 OMB Unique Project Identifier #REF!
 Project Name #REF!

(FY 2011) PIA: Final Signatures

Facility Name: #REF!

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

#REF!	Dee Tyner	404-828-5211	Dee.Tyner@va.gov
-------	-----------	--------------	--

Health Eligibility Center
Digitally signed by Health Eligibility Center
DN: cn=Health Eligibility Center, email=Dee.Tyner@va.gov, o=Department of Veterans Affairs
Date: 2011.02.16 12:04:18 -05'00'

#REF!	Michael Francis	404-828-5319	Michael.Francis@va.gov
-------	-----------------	--------------	--

MICHAEL A FRANCIS
Digitally signed by MICHAEL A FRANCIS
DN: o=Department of Veterans Affairs, ou=Dept of Veterans Affairs, Internal Staff, ou=www.vetsaff.com, postalCode=22030, cn=Michael A Francis, email=michaelafrancis@va.gov
Date: 2011.02.16 13:33:49-05'00'

#REF!	Chuck Shrader	404-828-5200	Chuck.Shrader@va.gov
-------	---------------	--------------	--


Digitally signed by Chuck Shrader
Date: 2011.02.16 20:56:35 -05'00'

#REF!	Tony Guagliardo	404-828-5300	Tony.Guagliardo@va.gov
-------	-----------------	--------------	--


#REF! Tyrone Wood

#REF!	Tyrone Wood	404-828-5200	Tyrone.Wood@va.gov
-------	-------------	--------------	--

Date of Report: #REF!
OMB Unique Project Identifier #REF!
Project Name #REF!

The Signature Process:

- Complete the PIA form.
- Name the PIA Excel FORM ["FY11-Region # - Facility Name - Facility # -Date(mmddyyyy).xls"]
 - Example: "FY11-Region3-Lexington VAMC-596-10302008.xls"
- Submit the completed PIA Excel form to SMART Database.
- Fix errors the reviewers sent back, rename the file and submit to SMART Database
- If no errors, convert form into PDF with Nuance PDF Professional.
- Name the PIA PDF form ["FY11-Region #-Facility Name- Facility # -Date(mmddyyyy).xls"]
- Obtain digital signatures on the "Final Signatures tab"
- Submit signed PIA PDF form to the SMART Database.