

## **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](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](mailto:christina.pettit@va.gov) to received full credit for submission.

## (FY 2011) PIA: System Identification

Program or System Name: REGION3>VHA>VISN7>Central Alabama Veterans Health Care System> 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 2300 FTE) necessary to operate the system. VistA-Legacy is a clientserver 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 life cycle.

Facility Name: Central Alabama Veterans Health Care System (CAVHCS)

Title: Name:

Privacy Officer: Michael Muse

Information Security Officer: Patricia Cross

System Owner/ Chief Information Officer: Rhoda Tyson

Information Owner: Michael Lay

Other Titles:

Person Completing Document: Linda Feaselman

Other Titles: Vista Systems Manager Linda Feaselman

Date of Last PIA Approved by VACO Privacy Services: 07/2008

Date Approval To Operate Expires: 8/29/2011

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:

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.

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): 03/2011

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

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

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

---

Phone:	Email:
(334) 727-0550 x3322	<a href="mailto:michael.muse@va.gov">michael.muse@va.gov</a>
(334) 273-6263 x4507	<a href="mailto:patricia.cross@va.gov">patricia.cross@va.gov</a>
(334) 727-0550 x3784	<a href="mailto:rhoda.tyson@va.gov">rhoda.tyson@va.gov</a>
(734) 222-4333	<a href="mailto:michael.lay@va.gov">michael.lay@va.gov</a>

(334) 799-0907 [linda.feaselman@va.gov](mailto:linda.feaselman@va.gov)  
(334) 799-0907 [linda.feaselman@va.gov](mailto:linda.feaselman@va.gov)

---

369090  
Operations/Maintenance

24 years

Yes

Yes

---

---



g work



## (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.

---

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

1. All System of Record Identifier(s) (number):
  2. Name of the System of Records:
  3. Location where the specific applicable System of Records Notice may be accessed (include the URL):
- 

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

---

Does the System of Records Notice require modification or updating?

---

Is PII collected by paper methods?

Is PII collected by verbal methods?

Is PII collected by automated methods?

Is a Privacy notice provided?

Proximity and Timing: Is the privacy notice provided at the time of data collection?

Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

---

---

Yes

---

79VA19

Veterans Health Information Systems and Technology  
Architecture (VistA) Records, VA

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

---

Yes

---

No

---

***(Please Select Yes/No)***

Yes

Yes

Yes

Yes

Yes

Yes

Yes

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	Eligibility, Benefits, Healthcare	All	All
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Eligibility, Benefits	All	All
Service Information	ALL	Eligibility, Benefits	All	All
Medical Information	ALL	Healthcare, Benefits	All	All
Criminal Record Information	Paper & Electronic	Eligibility, Billing	All	All
Guardian Information	Paper & Electronic	Healthcare	Verbal & Written	Verbal & Written
Education Information	Paper & Electronic	Healthcare, Billing	Verbal & Written	Verbal & Written
Benefit Information	Paper & Electronic	Eligibility, Benefits, Employment	All	All
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Mandatory	
Service Information	Yes	Veteran	Mandatory	

Medical Information	Yes	Veteran	Mandatory	
Criminal Record Information	Yes	VA Files / Databases (Identify file)	Mandatory	Fugitive Felon Program
Guardian Information	Yes	Veteran	Mandatory	
Education Information	Yes	Veteran	Mandatory	
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	VBA
Other (Explain)				
Other (Explain)				
Other (Explain)				

(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VA Regional Office (VARO) (Atlanta and Montgomery)	Yes	VARO: SSN, Date of Birth and sex for the adjudication of VA	Both PII & PHI	VHA Handbooks 1605.1 and VHA 1605.2
Other Veteran Organization	DAV Hospital Service Coordinator	Yes	Read Only access to the patient medical record	PHI	VHA Handbooks 1605.1 and VHA 1605.2
Other Federal Government Agency	Social Security Administration; Internal Revenue Service (IRS); Centers for Disease Control (CDC)	No	VARO and SSA: Name, SSN, Date of Birth and sex for the adjudication of VA beneficiary claims, SSA disability determination, and income verification; IRS: PII for verification of income for billing purposes; CDC: PII and PHI for healthcare reporting	Both PII & PHI	VHA Handbooks 1605.1 and VHA 1605.2
State Government Agency		No		N/A	
Local Government Agency		No		N/A	
Research Entity		No		N/A	
Other Project / System	Federal Bidirectional Health Information Exchange (FHIE/BHIE)	Yes	PII and PHI for the provision of healthcare to veterans and active duty soldiers	Both PII & PHI	VHA Handbooks 1605.1 and VHA 1605.2
Other Project / System					
Other Project / System					

(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? 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:

---

## (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?

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 and verified with veteran.

---

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

Answer: Clinical data is not removed. Administrative data is updated with each 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 at the treating facility for three years. If no activity is recorded in three years the record is converted to inactive. If inactive for one year, the record is transferred to the Federal Record storage recalled records are destroyed 72 years after retirement or 75 years after last episode of care. Record is maintained for a document of record.

---

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

Answer:[http://vaww1.va.gov/vapubs/viewPublication.asp?Pub\\_ID=19&FType=2](http://vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&FType=2), VA Handbook 6300.1, [http://vaww1.va.gov/vapubs/viewPublication.asp?Pub\\_ID=19&FType=2](http://vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&FType=2) , and VHA Records Control Schedule(RCS) 10-1, [http://vaww1.va.gov/VHA publications/rcs10/rcs10-1.pdf](http://vaww1.va.gov/VHA%20publications/rcs10/rcs10-1.pdf). The final, consolidated, electronic version of a Patient Medical Record, including information migrated from interim electronic information systems, electronic medical equipment, or information entered directly into the patient medical record information system is destroyed/deleted 75 years after the last episode of patient care, in accordance with RCS 10-1, XLIII, 2.b., Electronic Final Version of Health Record. Veterans Health Administration (VHA) RCS 10-1 is the main authority for the retention disposition of VHA records. It provides a brief description of the records and states the retention and disposition requirements. It also provides the National Archives and Records Administration (NARA) disposition authorities or the General Records Schedules (GRS) authorities, whichever is appropriate for the records. In addition to program and services sections, the RCS 10-1 contains a General and Administrative (G&A) Section for records common to several offices and services. Retention periods for data stored vary according to the type of records. Data owners are responsible for ensuring they follow the records retention periods outlined in RCS 10-1. Answer: Data is maintained in accordance with VA Directive 6300, [http://vaww1.va.gov/vapubs/viewPublication.asp?Pub\\_ID=19&FType=2](http://vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&FType=2), VA Handbook 6300.1.

---

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 10-1, Item XLIII, 2.b. (Page 190). At the present time, VistA Imaging retains all images.

---

Where are these procedures documented?

Answer: VA Handbook 6300; Records Control Schedule 10-1

---

How are data retention procedures enforced?

Answer: VA Records Control Schedule 10-1 (page8): Records Management Responsibilities: The Health Information Resources Service (HIRS) is responsible for developing policies and procedures for effective and efficient records management throughout VHA. In addition, HIRS acts as the liaison between VHA and National Archives and Records Administration (NARA) on issues pertaining to records management practices and procedures. Field records officers are responsible for records management activities at their facilities. Program officials are responsible for creating, maintaining, protecting, and disposing of records in their program area in accordance with NARA regulations and VA policy. All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures for the disposition of Records.

---

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

---

*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?

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

Answer:

---

---

No

---

---

---

---

---

---

---

---

---

---

---

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Yes

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

No

\_\_\_\_\_

## (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 a

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented

---

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

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

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

If 'No' to any of the 3 questions above, please describe why:

Answer:

---

Is adequate physical security in place to protect against unauthorized access?

If 'No' please describe why:

Answer:

---

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

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

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

- Air Conditioning Failure
- Chemical/Biological Contamination
- Blackmail
- Bomb Threats
- Burglary/Break In/Robbery
- Cold/Frost/Snow
- Communications Loss
- Computer Intrusion
- Computer Misuse
- Data Destruction
- Data Disclosure
- Data Integrity Loss
- Denial of Service Attacks
- Earthquakes
- Eavesdropping/Interception
- Errors (Configuration and Data Entry)
- Fire (False Alarm, Major, and Minor)
- Flooding/Water Damage
- Fraud/Embezzlement
- Hardware Failure
- Identity Theft
- Malicious Code
- Power Loss
- Sabotage/Terrorism
- Storms/Hurricanes
- Substance Abuse
- Theft of Assets
- 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) : System and communication protection (SC); and system and information integrity (SI)

### PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information

Answer: Review and reconciliation of local policy settings versus settings related in SSP.

The potential impact is **low** if the loss of integrity could be expected to have an adverse effect on operations, assets or individuals.

The potential impact is **high** if the loss of availability could be expected to have a 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 an adverse effect on operations, assets or individuals.

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 confidentiality could be expected to have a 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 an 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)

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 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, availability, and information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; information protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and component security; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exception is provided in the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

---

*Please add additional controls:*

---

---

appropriately secured.      Yes

d those controls..      Yes

---

Yes

Yes

Yes

---

Yes

---

- 
- Hardware Failure
  - Identity Theft
  - Malicious Code
  - Power Loss
  - Sabotage/Terrorism
  - Storms/Hurricanes
  - Substance Abuse
  - Theft of Assets
  - Theft of Data
  - Vandalism/Rioting

---

Personnel Security

Physical and Environmental Protection

Risk Management    d to have a serious

ected to have a limited

e expected to have a severe or  
uals.

uld be expected to have a

expected to have a limited

be expected to have a severe  
uals.

could be expected to have a

e expected to have a limited

---

---

ty, and availability of VA  
ress and training; audit and  
incident response; maintenance;  
mmunications protection; and  
is have been allowed based on

---

---

**(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

<b>Which of these are sub-components of your system?</b>
--

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?**

Yes ASISTS	Yes	Beneficiary Travel	Yes Accounts Receivable	Yes
No Bed Control	Yes	Care Management	Yes ADP Planning (PlanMan)	Yes
Yes CAPRI	Yes	Care Tracker	Yes Bar Code Med Admin	Yes
Yes CMOP	Yes	Clinical Reminders	Yes Clinical Case Registries	Yes
Yes Dental	Yes	CPT/ HCPCS Codes	Yes Clinical Procedures	Yes
Yes Dietetics	Yes	DRG Grouper	Yes Consult/ Request Tracking	Yes
Yes Fee Basis	Yes	DSS Extracts	Yes Controlled Substances	Yes
Yes GRECC	no	Education Tracking	Yes Credentials Tracking	Yes
Yes HINQ	Yes	Engineering	Yes Discharge Summary	Yes
Yes IFCAP	Yes	Event Capture	Yes Drug Accountability	Yes
Yes Imaging	Yes	Extensible Editor	Yes EEO Complaint Tracking	Yes
Yes Kernel	Yes	Health Summary	Yes Electronic Signature	Yes
Yes Kids	Yes	Incident Reporting	Yes Event Driven Reporting	Yes
Yes Lab Service	Yes	Intake/ Output	Yes External Peer Review	Yes
Yes Letterman	Yes	Integrated Billing	Yes Functional Independence	Yes
Yes Library	Yes	Lexicon Utility	Yes Gen. Med. Rec. - I/O	Yes
Yes Mailman	Yes	List Manager	Yes Gen. Med. Rec. - Vitals	Yes
Yes Medicine	Yes	Mental Health	Yes Generic Code Sheet	Yes
Yes MICOM	Yes	MyHealthEVet	Yes Health Level Seven	Yes
Yes NDBI	Yes	National Drug File	Yes Hospital Based Home Care	Yes
Yes NOIS	Yes	Nursing Service	Yes Inpatient Medications	Yes
Yes Oncology	Yes	Occurrence Screen	Yes Integrated Patient Funds	Yes
Yes PAID	Yes	Patch Module	Yes MCCR National Database	Yes
Yes Prosthetics	Yes	Patient Feedback	Yes Minimal Patient Dataset	Yes
Yes QUASER	Yes	Police & Security	Yes National Laboratory Test	No
Yes RPC Broker	Yes	Problem List	Yes Network Health Exchange	Yes

Yes SAGG	Yes	Progress Notes	Yes	Outpatient Pharmacy	Yes
Yes Scheduling	Yes	Record Tracking	Yes	Patient Data Exchange	Yes
Yes Social Work	Yes	Registration	Yes	Patient Representative	Yes
Yes Surgery	Yes	Run Time Library	Yes	PCE Patient/ HIS Subset	Yes
Yes Toolkit	Yes	Survey Generator	No	Security Suite Utility Pack	Yes
No Unwinder	Yes	Utilization Review	Yes	Shift Change Handoff Tool	No
Yes VA Fileman	Yes	Visit Tracking	Yes	Spinal Cord Dysfunction	Yes
Yes VBECS	Yes	VistALink Security	Yes	Text Integration Utilities	Yes
Yes VDEF	Yes	Women's Health	Yes	VHS & RA Tracking System	Yes
Yes VistALink			Yes	Voluntary Timekeeping	Yes

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

Name	Bed Board Management System
Description	Provides ward specific bed utilization information to assist with bed control
Comments	
Is PII collected by this minor application?	
Does this minor application store PII?	
If yes, where?	Dedicated Server
Who has access to this data?	Limited IT Personnel, Limited Clinical Staff

Name	Automated Access Request (AAR)
Description	Allows designated individuals to enter local and remote requests for system access. Requests are routed through an approval process prior to accounts being created.
Comments	
Is PII collected by this minor application?	
Does this minor application store PII?	
If yes, where?	Vista
Who has access to this data?	HR Personnel

Name	Health Summary Contingency
------	----------------------------

Description

Designated encrypted workstations are located in ward and patient treatment areas to permit patient clinical information access if the main computer systems are unavailable

Comments

Is PII collected by this minor application?

Does this minor application store PII?

If yes, where? Dedicated Contingency PCs (Encrypted)

Who has access to this data? IT Personnel, Limited Clinical Staff

---

---

Adverse Reaction Tracking  
Authorization/ Subscription  
  
Auto Replenishment/ Ward Stock  
  
Automated Info Collection Sys  
  
Automated Lab Instruments  
  
Automated Med Info Exchange  
  
Capacity Management - RUM  
  
Capacity Management Tools  
  
Clinical Info Resource Network  
  
Clinical Monitoring System  
  
Enrollment Application System  
  
Equipment/ Turn-in Request  
  
Gen. Med.Rec. - Generator  
  
Health Data and Informatics  
  
ICR - Immunology Case Registry  
  
Income Verification Match  
  
Incomplete Records Tracking  
  
Interim Mangement Support  
  
Master Patient Index VistA  
Missing Patient Reg (Original) A4EL  
  
Order Entry/ Results Reporting  
  
PCE Patient Care Encounter  
  
Pharmacy Benefits Mangement  
  
Pharmacy Data Management  
  
Pharmacy National Database  
  
Pharmacy Prescription Practice

Quality Assurance Integration

Quality Improvement Checklist

Radiology/ Nuclear Medicine

Release of Information - DSSI

Remote Order/ Entry System

Utility Management Rollup

CA Verified Components - DSSI

Vendor - Document Storage Sys

Visual Impairment Service Team ANRV

Voluntary Timekeeping National

n the list above. Please provide name,

YES  
YES

YES  
YES

YES  
YES

(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: REGION3>VHA>VISN7>Central Alabama Veterans Health Care System> Vista - VMS

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

Privacy Officer:	Michael Muse	(334) 727-0550 x3322	michael.muse@va.gov
------------------	--------------	-------------------------	---------------------

Digital Signature Block

Information Security Officer:	Patricia Cross	(334) 727-0550 x4507	patricia.cross@va.gov
-------------------------------	----------------	-------------------------	-----------------------

Digital Signature Block 

System Owner/ Chief Information Officer:	Rhoda Tyson	(334) 727-0550 x3784	rhoda.tyson@va.gov
--	-------------	-------------------------	--------------------

Digital Signature Block

Information Owner:	Michael Lay	(734) 222-4333	michael.lay@va.gov
--------------------	-------------	----------------	--------------------

Digital Signature Block

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

Digital Signature Block

Date of Report: 3/22/11

OMB Unique Project Identifier 0

Project Name REGION3>VHA>VISN7>Central Alabama Veterans Health Care System> Vista - VMS

Project Name System> Vista - VMS