

## **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: REGION 3> VHA> VISN 8> Miami VAHS> VISTA-VMS  
 OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-01-11-01-1180-00

The VistA system is designed to operate as a fully integrated clinical and administrative information source. It processes clinical information, information covered by the Privacy Act & HIPAA, PHI/ePHI, financial records, and all other data necessary to run a tertiary medical center. All clinical and most administrative functions within the physical confines of the VISN8 utilize the VistA Alpha cluster to process clinical, financial, or administrative data. All external organizations which access a local Alpha node must be authenticated by access and verify codes or by domain transmission scripts for electronic mail. Examples of these organizations include VBA Regional Office, Form, HINQ, all VA facilities throughout the country sending electronic mail, Medical Cost Recovery vendors and transcription vendors. The native operating system of the Alpha cluster is VMS. Cache is a programming language that runs on top of VMS. Using the Cache environment, the VA's VistA program exists with all attendant menus, parameters, and data. Cache is the only application inhabiting the Alpha cluster.

Description of System/  
 Application / Program:

Facility Name: Miami VAHS

Title:	Name:	Phone:	Email:
Privacy Officer:	Cristina M. Gonzalez	305-575-7239	<a href="mailto:cristina.gonzalez@va.gov">cristina.gonzalez@va.gov</a>
Information Security Officer:	Carl Lindsey/Tony Mateo	303-575-3361	<a href="mailto:carl.lindsey@va.gov">carl.lindsey@va.gov</a>
System Owner/ Delegation of Authority	Micheal Lay		
Other Titles: CIO	Jason Gray		<a href="mailto:jason.gray2@va.gov">jason.gray2@va.gov</a>
Other Titles:			

Person Completing

Document: Tony Mateo [tony.mateo@va.gov](mailto:tony.mateo@va.gov)

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: 04/2009

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: 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. 30 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): 04/2011

**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 - VMS

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?

Yes

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

Is PII collected by paper methods?

Yes

Is PII collected by verbal methods?

Yes

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

Yes

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

Yes

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

Yes

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

Yes

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

Yes

**(FY 2011) PIA: Notice**

Please fill in each column for the data types selected.

<b>Data Type</b>	<b>Collection Method</b>	<b>What will the subjects be told about the information collection?</b>	<b>How is this message conveyed to them?</b>	<b>How is a privacy notice provided?</b>
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Electronic/File Transfer	Will only collect minimum necessary	All	Written
Family Relation (spouse, children, parents, grandparents, etc)	Electronic/File Transfer	Collected for emergency purposes	Written	Written
Service Information	Electronic/File Transfer	collected for the purpose of determining eligibility	All	All
Medical Information	ALL	collected to provide health care	All	All
Criminal Record Information	Electronic/File Transfer	will only collect minimum necessary	All	All
Guardian Information	N/A			
Education Information	N/A			
Benefit Information	Electronic/File Transfer	collected for the purpose of determining eligibility	All	All
Other (Explain)				

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

Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory
Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory
Criminal Record Information	Yes	Local Agency (Identify)	Voluntary
Guardian Information	Yes	Veteran	Voluntary
Education Information	Yes	Veteran	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/Regional Office	Yes	treatment and demographic for benefits determination. Regional Council:	Both PII & PHI	VHA1605.1 and VHA 1605.2 VA Handbooks and VA handbook 6500, local privacy and security policies.
Other Veteran Organization		No			
Other Federal Government Agency	DOD, CDC, HHS, SSA, and Congressional inquiries	Yes	Congressional inquiries accompanied by patient authorization; various information including appointment dates, treatment, medical documentation, bills, co-pays. There is certain VA patient data that is shared with DoD through the information exchange program. In addition, certain clinical data is shared with CDC as is certain data shared with HHS and SSA	Both PII & PHI	VHA1605.1 and VHA 1605.2 VA Handbooks and VA handbook 6500, local privacy and security policies.

State Government Agency	Veterans Home	Yes	Veterans Home inquiries accompanied by patient authorization; data shared can be various information including appointment dates, treatment, medical documentation, bills, copays. The purpose is to fulfill a duly authorized request.	Both PII & PHI	VHA1605.1 and VHA 1605.2 VA Handbooks and VA handbook 6500, local privacy and security policies.
Local Government Agency	Corner's Office	Yes	death certificates, department of transportation for handicap verification, dept of family services, CDC.	PII	VHA1605.1 and VHA 1605.2 VA Handbooks and VA handbook 6500, local privacy and security policies.
Research Entity					
Other Project / System					
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:	<input checked="" type="checkbox"/> Through a Written Request <input checked="" type="checkbox"/> Submitted in Person <input type="checkbox"/> Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	Yes

### (FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?	Yes
---	-----

Drug/Alcohol Counseling       Mental Health       HIV

if yes, please check all that apply:

Research     Sickle Cell     Other (Please Explain)

---

Describe process for authorizing access to this data.

Answer: Before authorizing access to the Data users require Cyber Security and Privacy training. After that they get that mandatory training annually .

---

## (FY 2011) PIA: Program Level Questions

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

No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

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

Forms input fields used provide the limit of data collection. Can be collected via interview process, forms submitted, or telephone contacts.

How is data checked for completeness?

Answer: The process of data review is that the staff review and compare input information to paper forms. An additional opportunity to verify is during the patient registration process.

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

Answer: Interview; the process of asking questions, and concurrence when changes are requested help ensure data is current.

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

Answer: New data is compared with printed form or via patient verification. The process is to review the new data and make a comparison with the old data – then verify for correctness.

*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 for a period of 75 years according to IAW VA Records Control Schedule 10-1.

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

Answer: Demographic information is updated as applications for care are submitted and retained IAW VA RCS 10-1.

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 RCS 10-1.

Where are these procedures documented?

Answer: VA Handbook 6300; RCS 10-1

How are data retention procedures enforced?

Answer: VA Records Center and Vault (RC&V) will let us know when eligible records are up for destruction, a notice is sent out to the Facility Record Officer; this is all according VA RCS 10-1 and 36 CFR 1228.58

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: OCIS is responsible for the establishment of directives, policies, procedures which are consistent with the provisions of FISMA as well as guidance issued by OMB, NIST, and other requirements that VISTA-VMS is subject to. SMART, OI&T, ITOC, and EoC rounds combine to ensure requirements are measured and either met or remediated through new procedures or system modifications.

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

- |  |  |   |
|--|--|---|
| <input checked="" type="checkbox"/> Air Conditioning Failure | <input type="checkbox"/> Data Disclosure                       | <input checked="" type="checkbox"/> Hardware Failure  |
| <input type="checkbox"/> Chemical/Biological Contamination   | <input 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 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 checked="" type="checkbox"/> Storms/Hurricanes |
| <input type="checkbox"/> Communications Loss                 | <input type="checkbox"/> Fire (False Alarm, Major, and Minor)  | <input type="checkbox"/> Substance Abuse              |
| <input type="checkbox"/> Computer Intrusion                  | <input 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            |

Data Destruction

Fraud/Embezzlement

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 type="checkbox"/> Contingency Planning              | <input checked="" type="checkbox"/> Personnel Security                    |
| <input checked="" type="checkbox"/> Audit and Accountability                  | <input type="checkbox"/> Identification and Authentication | <input checked="" type="checkbox"/> Physical and Environmental Protection |
| <input checked="" type="checkbox"/> Awareness and Training                    | <input type="checkbox"/> Incident Response                 | <input type="checkbox"/> Risk Management                                  |
| <input type="checkbox"/> Certification and Accreditation Security Assessments |  |   |
| <input 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 is a national level program and is governed by existing policies and procedures; the PIA was not used to identify any additional collection issues, no changes to the system, and no documentation changes or procedure changes.

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization?  
**(Choose One)**

- |   |
|---|
| <input checked="" type="checkbox"/> The potential impact is <b>high</b> if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. |
| <input type="checkbox"/> The potential impact is <b>moderate</b> if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.                       |
| <input type="checkbox"/> The potential impact is <b>low</b> if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.                            |

Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?  
**(Choose One)**

- |  |
|--|
| <input checked="" type="checkbox"/> The potential impact is <b>high</b> if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. |
| <input type="checkbox"/> The potential impact is <b>moderate</b> if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals.                       |
| <input type="checkbox"/> The potential impact is <b>low</b> 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

- |  |
|--|
| <input checked="" type="checkbox"/> The potential impact is <b>high</b> if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. |
| <input type="checkbox"/> The potential impact is <b>moderate</b> if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals.                       |

the system or organization?

**(Choose One)**



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

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

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

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	x	Beneficiary Travel	Accounts Receivable	Adverse Reaction Tracking
Bed Control		Care Management	ADP Planning (PlanMan)	Authorization/ Subscription
CAPRI	x	Care Tracker	x Bad Code Med Admin	Auto Replenishment/ Ward Stock
CMOP	x	Clinical Reminders	Clinical Case Registries	Automated Info Collection Sys
x Dental	x	CPT/ HCPCS Codes	x Clinical Procedures	Automated Lab Instruments
Dietetics		DRG Grouper	x Consult/ Request Tracking	Automated Med Info Exchange
x Fee Basis	x	DSS Extracts	x Controlled Substances	Capacity Management - RUM
GRECC		Education Tracking	Credentials Tracking	Capacity Management Tools
HINQ	x	Engineering	x 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	x Equipment/ Turn-in Request
x Kids		Incident Reporting	x Event Driven Reporting	Gen. Med.Rec. - Generator
x Lab Service		Intake/ Output	External Peer Review	x Health Data and Informatics
Letterman	x	Integrated Billing	Functional Independence	ICR - Immunology Case Registry
Library		Lexicon Utility	Gen. Med. Rec. - I/O	Income Verification Match
x Mailman		List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine		Mental Health	Generic Code Sheet	Interim Mangement Support
MICOM	x	MyHealthEVet	Health Level Seven	Master Patient Index Vista
NDBI		National Drug File	Hospital Based Home Care	Missing Patient Reg (Original) A4EL
NOIS	x	Nursing Service	Inpatient Medications	Order Entry/ Results Reporting
x Oncology		Occurrence Screen	Integrated Patient Funds	PCE Patient Care Encounter
x PAID	x	Patch Module	MCCR National Database	Pharmacy Benefits Mangement
x Prosthetics	x	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
SAGG		Progress Notes	x Outpatient Pharmacy	Quality Assurance Integration
x Scheduling	x	Record Tracking	x Patient Data Exchange	Quality Improvement Checklist
Social Work	x	Registration	Patient Representative	Radiology/ Nuclear Medicine
Surgery		Run Time Library	PCE Patient/ HIS Subset	Release of Information - DSSI
Toolkit		Survey Generator	Security Suite Utility Pack	x 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
x VBECS	x	VistALink Security	Text Integration Utilities	Vendor - Document Storage Sys
VDEF		Women's Health	VHS & RA Tracking System	Visual Impairment Service Team ANRV
x 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

## (FY 2011) PIA: Final Signatures

Facility Name: REGION 3> VHA> VISN 8> Miami VAHS> VISTA-VMS

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

Privacy Officer:	Cristina M. Gonzalez	305-575-7239	cristina.gonzalez@va.gov
------------------	----------------------	--------------	--------------------------

Digital Signature Block
-------------------------

Information Security Officer:	Carl Lindsey/Tony Mateo	303-575-3361	carl.lindsey@va.gov
-------------------------------	-------------------------	--------------	---------------------

Digital Signature Block
-------------------------

System Owner/ Delegation of Authority	Micheal Lay	0	0
---------------------------------------	-------------	---	---

Digital Signature Block
-------------------------

Other Titles: CIO	Jason Gray	0	jason.gray2@va.gov
-------------------	------------	---	--------------------

Digital Signature Block
-------------------------

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

Digital Signature Block
-------------------------

Date of Report:	4/14/11
OMB Unique Project Identifier	029-00-01-11-01-1180-00
Project Name	REGION 3> VHA> VISN 8> Miami VAHS> VISTA-VMS