

## **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 07 > Tuscaloosa VAMC > VistA - VMS  
 OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-01-11-01-1180-00

The records include information concerning current and former employees, applicants for employment, trainees, contractors, sub- contractors, contract personnel, students, providers and consultants, patients and members of their immediate family, volunteers, maintenance personnel, as well as individuals working collaboratively with the VA. Records are maintained at each VA health care facility. Records are maintained on paper, microfilm, magnetic tape, disk, or laser optical media. In most cases, copies of back-up computer files are maintained at off-site locations. The records and information may be used for statistical analysis to produce various management, workload tracking and follow-up reports; to track and evaluate the ordering and delivery of equipment, services and patient care; the planning, distribution and utilization of resources; the possession and/or use of equipment or supplies; the performance of vendors, equipment, and employees; and to provide clinical and administrative support to patient medical care. The data may be used for research purposes. The data may be used also for such purposes as assisting in the scheduling of tours of duties and job assignments of employees; the scheduling of patient treatment services, including nursing care, clinic appointments, surgery, diagnostic and therapeutic procedures; the repair and maintenance of equipment and for follow-up to determine that the actions were accomplished and to evaluate the results; the registration of vehicles and the assignment and utilization of parking spaces; to plan, schedule, and maintain rosters of patients, employees and others attending or participating in sports, recreational or other events; for audits, reviews, and investigations conducted by staff of the health care facility, the Network Directors Office, VA Central Office, and the VA Office of Inspector General; for quality assurance audits, reviews, investigations and inspections; for law enforcement investigations; and for personnel management, evaluation and employee ratings, and performance evaluations. The VistA system boundary includes RPC Broker, CPRS, VistA Kernal, VistA Database, VistA Platform (Operating System and DBMS), Pharmacy Re-Engineering System, and any applicable VistA Applications covered in this PIA.

Description of System/ Application/ Program:

Facility Name:	Tuscaloosa VAMC		
<b>Title:</b>	<b>Name:</b>	<b>Phone:</b>	<b>Email:</b>
Privacy Officer:	Quin Denton	205-554-2885	<a href="mailto:quin.denton@va.gov">quin.denton@va.gov</a>
Information Security Officer:	Alicia Marshall	205-554-3652	<a href="mailto:alicia.marshall@va.gov">alicia.marshall@va.gov</a>
System Owner/ Chief Information Officer:	Antonia Mohamed	205-554-2020	<a href="mailto:antonia.mohamed@va.gov">antonia.mohamed@va.gov</a>
Information Owner:	Michael Lay	734-222-4333	<a href="mailto:michael.lay@va.gov">michael.lay@va.gov</a>
Other Titles: VistA System Manager	John Williams	205-554-2870	<a href="mailto:john.williams8@va.gov">john.williams8@va.gov</a>
Person Completing Document:	Quin Denton	205-554-2885	<a href="mailto:quin.denton@va.gov">quin.denton@va.gov</a>
Other Titles:			

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	02/2008
Date Approval To Operate Expires:	08/2011
What specific legal authorities authorize this program or system:	Title 38, United States Code, section 7301(a)
What is the expected number of individuals that will have their PII stored in this system:	85,000
Identify what stage the System / Application / Program is at:	Operations/Maintenance
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.	29 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):	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)**

### (FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.

Yes

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

1. All System of Record Identifier(s) (number):

79VA19

2. Name of the System of Records:

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

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

[http://www.rms.oit.va.gov/SOR\\_Records/79VA19.asp](http://www.rms.oit.va.gov/SOR_Records/79VA19.asp)

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

Yes

Does the System of Records Notice require modification or updating?

No

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

Is PII collected by paper methods?

Yes

Is PII collected by verbal methods?

Yes

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

Yes

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

Yes

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

Yes

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

Yes

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

Yes

## (FY 2011) PIA: Notice

Please fill in each column for the data types selected.

<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)	ALL	Information is collected and used in accordance with the notice of privacy practices and HIPAA.	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Information is collected and used in accordance with the notice of privacy practices and HIPAA.	Written	Written
Service Information	ALL	Information is collected and used in accordance with the notice of privacy practices and HIPAA.	Written	Written
Medical Information	ALL	Information is collected and used in accordance with the notice of privacy practices and HIPAA.	Written	Written
Criminal Record Information	N/A			
Guardian Information	ALL	Information is collected and used in accordance with the notice of privacy practices and HIPAA.	Written	Written
Education Information	ALL	Information is collected and used in accordance with the notice of privacy practices and HIPAA.	Written	Written
Benefit Information	ALL	Information is collected and used in accordance with the notice of privacy practices and HIPAA.	Written	Written
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	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	
Service Information	Yes	Veteran	Mandatory	Verified through VA HEC
Medical Information	Yes	Veteran	Voluntary	Data also comes from the Master Patient Index, VistA Web, and Remote Data
Criminal Record Information	No			
Guardian Information	Yes	Veteran	Voluntary	Data also comes from Power of Attorney (state and local)
Education Information	Yes	Other (Explain)	Voluntary	Collected from Employees
Benefit Information	Yes	Veteran	Mandatory	Verified through VA HEC
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	Veterans Affairs	Yes	Continuity of Care, Benefits	Both PII & PHI	VHA Privacy Handbook 1605.1
Other Veteran Organization		No			
Other Federal Government Agency	DoD	No	Health Care	Both PII & PHI	Patient signs waiver for info to be viewed through VistA Web and Remote Data
State Government Agency		No			
Local Government Agency		No			
Research Entity	wocs? Sponsor, affiliates	Yes	Research	Both PII & PHI	VHA Handbook 1200.05
Other Project / System	Quest Diagnostics	Yes	To deliver the electronic ordering of patient lab tests to Quest Diagnostics, who in turn, delivers the electronic results back to the Dept. of VA.	Both PII & PHI	MOU/ISA
Other Project / System	ScriptPro	Yes	When required, ScriptPro technical support services will download sensitive patient health information for the purposes of troubleshooting or diagnosing a problem reported by the pharmacy user.	PHI	MOU/ISA

---

### (FY 2011) PIA: Access to Records

---

Does the system gather information from another system? Yes

Please enter the name of the system: HINQ

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? Yes

---

if yes, please check all that apply:

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

---

Describe process for authorizing access to this data.  
Must be approved by the IRB and R&D committee.

---

## (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: In accordance with the notice of privacy practices and HIPAA.

How is data checked for completeness?

Answer: Data validation committee and system input validation checks.

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

Answer: Verbal confirmation at each visit.

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

Answer: Data is reviewed by staff, compared to paper forms, and verified with Next of Kin. Internal audits are conducted on data for accuracy. 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: VA mandates storage of patient record information for 75 years (after patient death) whether in hard copy or electronic format. Clinical information is retained in accordance with VA Records Control Schedule 10-1. Demographic information is updated as applications for care are submitted and retained in accordance with VA Records Control Schedule 10-1.

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

Answer: Readily accessible use of patient records which contain sufficiently recorded information to serve as provision to assess and plan patient care, support diagnosis, and warrant treatment.

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

Answer: VA mandates storage of patient record information for 75 years (after patient death) whether in hard copy or electronic format. Legacy paper patient information is retired upon a schedule and shipped to any Federal Records Center through the nation. VistA/VistA Imaging retains all data.

Where are these procedures documented?

Answer: Center Memorandum Policy - Management of Medical Records Policy, VHA Handbook Privacy and Release of Information 1605.1, VHA Records Control Schedule (RCS) 10-1, Handbook 1907.01, Health Information Management and Health Records

How are data retention procedures enforced?

Answer: Center Memorandum Policy - Management of Medical Records Policy, VHA Handbook Privacy and Release of Information 1605.1, VHA Records Control Schedule (RCS) 10-1, Handbook 1907.01, Health Information Management and Health 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: Yes, retention schedule has been approved by NARA.

---

### **(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 Tuscaloosa VAMC VistA system adheres to all federal security requirements and procedures, to include but not limited to, FISMA, OMB, NIST, and any VA-specific policies and procedures.

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

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

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

Answer: (Other Controls)

## PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer: 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 **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
- The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

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

- The potential impact is **high** if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- The potential impact is **moderate** if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals.
- The potential impact is **low** if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.

Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization?  
**(Choose One)**

- The potential impact is **high** if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- The potential impact is **moderate** if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals.
- The potential impact is **low** if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.



---

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

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

---

*Please add additional controls:*

---

**(FY 2011) PIA: Additional Comments**

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

(FY 2011) PIA: VBA Minor Applications

**Which of these are sub-components of your system?**

Access Manager	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
Omicell	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?**

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

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

Name
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 07 > Tuscaloosa VAMC > VistA - VMS

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

Privacy Officer:	Quin Denton	205-554-2885	quin.denton@va.gov
------------------	-------------	--------------	--------------------

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

Information Security Officer:	Alicia Marshall	205-554-3652	alicia.marshall@va.gov
-------------------------------	-----------------	--------------	------------------------

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

System Owner/ Chief Information Officer:	Antonia Mohamed	205-554-2020	antonia.mohamed@va.gov
--	-----------------	--------------	------------------------

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

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

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

Other Titles: VistA System Manager	John Williams	205-554-2870	john.williams8@va.gov
------------------------------------	---------------	--------------	-----------------------

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

Date of Report: 1/0/00

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

REGION 3 > VHA > VISN 07 >

Project Name Tuscaloosa VAMC > VistA - VMS