



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

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)

## **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 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): 24VA19
2. Name of the System of Records: Patient Medical Records
3. Location where the specific applicable System of Records Notice may be accessed (include the URL): <http://www.vhaco.va.gov/privacy/SystemofRecords.htm>

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

Yes

Does the System of Records Notice require modification or updating?

No

*(Please Select Yes/No)*

- Is PII collected by paper methods? Yes
- Is PII collected by verbal methods? Yes
- Is PII collected by automated methods? Yes
- Is a Privacy notice provided? Yes
- Proximity and Timing: Is the privacy notice provided at the time of data collection? Yes
- Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used? Yes
- Authority: Does the privacy notice specify the effects of providing information on a voluntary basis? Yes
- Disclosures: Does the privacy notice specify routine use(s) that may be made of the information? Yes

**(FY 2011) PIA: Notice**

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal	Electronic/File Transfer	Will only collect minimum necessary	All	Written
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	N/A	N/A	N/A
Education Information	N/A	collected for the purpose of determining	All	All
Benefit Information	Electronic/File Transfer	eligibility	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		Veteran	Voluntary	
Contact Information (name, address, telephone, etc)	No	Veteran	Voluntary	

Family Relation (spouse, children, parents, grandparents, etc)

	No	Veteran	Voluntary
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory
Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory
Criminal Record Information	No	Veteran	Voluntary
Guardian Information	Yes	Veteran	Voluntary
Education Information	No	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					
Other Veteran Organization					
Other Federal Government Agency					
	IRS, SSA, & DOD	Yes	IRS, SSA, DOD data used for income verification to determine insurance, employability if third party collection is possible. Also used for determining eligibility for care; SSA for certification of death.	Both PII & PHI	VHA1605.1 and VHA 1605.2 VA Handbooks and VA handbook 6500, local privacy security policies.
State Government Agency					
Local Government Agency					
	Corner's Office	Yes	County Coroner offices for date of death, death certificate and circumstances.	PII	VHA1605.1 and VHA 1605.2 VA Handbooks and VA handbook 6500, local privacy and security policies.
Research Entity					
Other Project / System					
	University of Miami	No	We have Physician and Resident that work here at our Hospital	Both PII & PHI	handbook 6500, local privacy and security policies.
Other Project / System					

(FY 2011) PIA: Access to Records

Do data sharing and release 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?

No

- 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
  - Research
  - Sickle Cell
  - Other (Please Explain)
  - Mental Health
  - HIV

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?

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

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.)*

6. Program LVL Questions

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: 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 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 LAN is subject to. SMART, OI&T, ITOC, and EOC rounds combine to ensure requirements are met and procedures are in place.

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 checked="" type="checkbox"/> Flooding/Water Damage      | <input type="checkbox"/> Theft of Assets              |
| <input type="checkbox"/> Computer Misuse                     | <input type="checkbox"/> Fraud/Embezzlement                    | <input type="checkbox"/> Theft of Data                |
| <input 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
- Contingency Planning
- Personnel Security
- Audit and Accountability
- Identification and Authentication
- Physical and Environmental Protection
- Awareness and Training
- Incident Response
- Risk Management
- Certification and Accreditation Security Assessments
- Configuration Management
- 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: The LAN system is program that 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)

- 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

persons?

- 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 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:

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: Additional 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 (AMIME II)
Appraisal System	Benefits Delivery Network (BDN)	Automated Medical Information System (AMIS)290
ASSISTS	Centralized Property Tracking System	Automated Standardized Performance 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 & Pension 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	Personal 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	Personal Information Exchange System (PIES)
Insurance Self Service	Inventory Management System (IMS)	Personal 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 Entitlement Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Assistant	Service Member Records Tracking System
Omniceil	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
Sideaxis	State Benefits Reference System	Vocational Rehabilitation & Employment (VR&E) CH 31
Synquest	State of Case/Supplemental (SOC/SSOC)	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

9. VBA Minor Applications

VBA Data Warehouse	Telecare Record Manager	Web Automated Folder Processing System (WAFPS)
VBA Training Academy	VBA Enterprise Messaging System	Web Automated Reference Material System (WARMS)
Veterans Canteen Web	Veterans On-Line Applications (VONAPP)	Web Automated Verification of Enrollment
VIC	Veterans Service Network (VETSNET)	Web-Enabled Approval Management System (WEAMS)
VR&E Training Website	Web Electronic Lender Identification	Web Service Medical Records (WebSMR)
Web LGY		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.

<p>Name</p> <p>Description</p> <p>Comments</p> <p>Is PII collected by this min or application?</p> <p>Does this minor application store PII?</p> <p>If yes, where?</p> <p>Who has access to this data?</p>
--

<p>Name</p> <p>Description</p> <p>Comments</p> <p>Is PII collected by this min or application?</p> <p>Does this minor application store PII?</p> <p>If yes, where?</p> <p>Who has access to this data?</p>
--

<p>Name</p> <p>Description</p> <p>Comments</p> <p>Is PII collected by this min or application?</p> <p>Does this minor application store PII?</p> <p>If yes, where?</p> <p>Who has access to this data?</p>
--

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

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

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

(FY 2011) PIA: Minor Applications

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

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

(FY 2011) PIA: Final Signatures

Facility Name: REGION 3> VHA> VISN 8> Miami VAHS> LAN

Title: Name: Phone: Email:

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

  
JAPHET C. RIVERA  
ASSOCIATE DIRECTOR  
Digital Signature Block

Information Security Officer: Carl Lindsey / Tony Mateo 305-575-3361 carl.lindsey@va.gov

CARL J LINDSEY  
115488  
Digitally signed by CARL J LINDSEY 115488  
DN: dc=gov, dc=va, o=internal, ou=people,  
cn=CARL J LINDSEY 115488,  
c=CARL J LINDSEY 115488  
Date: 2011.04.29 15:04:39 -04'00'

System Owner/ Delegation of Authority Micheal Lay 0 0

  
Jason  
K Gray  
Digital Signature Block

Other Titles: CIO Jason Gray 305-575-6004 Jason.Gray2@va.gov

Digitally signed by Jason K Gray 279906  
DN: cn = Jason K Gray 279906 O = Internal OU = people  
Date: 2011.04.29 14:48:57 -05'00'

Jason  
K Gray  
Digital Signature Block

Other Titles: 0 0

Digital Signature Block

Date of Report: 4/14/11

OMB Unique Project Identifier 029-00-02-00-01-1120-00

REGION 3> VHA> VISN 8> Miami

Project Name VAHS> LAN