

## **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://vaww.privacy.va.gov/Privacy\\_Impact\\_Assessments.asp](http://vaww.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: CDCO>AITC>OI>VHIT> Spinal Cord Injury and Disorders  
 OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-02-00-01-1120-00

Description of System/ Application/ Program: Convert Legacy Spinal Cord Registry (command line based) to a client server platform with GUI enhanced capabilities. The primary objective is to produce an application that will enhance the SCID system of regional, coordinated primary and specialty health care.

### Facility Name:

Title:	Name:	Phone:	Email:
Privacy Officer:	Garnett Best	202-461-7474	<a href="mailto:Garnett.Best@va.gov">Garnett.Best@va.gov</a>
Information Security Officer:	Gerald Steward	210-616-8165	<a href="mailto:Gerald.Steward@va.gov">Gerald.Steward@va.gov</a>
System Owner/ Chief Information Officer:	John F. Quinn	512-326-6188	<a href="mailto:John.Quinn@va.gov">John.Quinn@va.gov</a>
Information Owner:	Jean Laubscher	206-277-1210	<a href="mailto:Jean.Laubscher2@va.gov">Jean.Laubscher2@va.gov</a>
Other Titles: Program Manager	Larry J. Clark	202-245-1663	<a href="mailto:Larry.Clark2@va.gov">Larry.Clark2@va.gov</a>
Person Completing Document:	Jean Laubscher	206-277-1210	<a href="mailto:Jean.Laubscher2@va.gov">Jean.Laubscher2@va.gov</a>

### Other Titles:

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY) 11/2010

Date Approval To Operate Expires: 09/2011

What specific legal authorities authorize this program or system: Title 38, United States Code, Sections 501 and 7304

What is the expected number of individuals that will have their PII stored in this system: Approximately 26,000 Veterans

Identify what stage the System / Application / Program is at: Implementation

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. 11/2010

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): 05/2011

**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?

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):

108VA11S

2. Name of the System of Records:

Spinal Cord Dysfunction - Registry (SCD-R) - VA

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

Federal Register -

<http://www.gpoaccess.gov/fr/search.html>

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?

*(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?

No

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

Yes

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

Yes

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

Yes

(FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Electronic/File Transfer	A Memorandum of Understanding exists between Veterans Health Administration Office of Information Health Project Support Office Testing Service and the Austin Automation Center dated October 24, 2006 which covers all phases of SCIDO development up through national deployment. VHA Contact - John Quinn. Patients are not informed of the various methods in which their data is stored at the regional or national level.		
Family Relation (spouse, children, parents, grandparents, etc)	N/A			
Service Information	Electronic/File Transfer			
Medical Information	Electronic/File Transfer			
Criminal Record Information				
Guardian Information	N/A			
Education Information	Electronic/File Transfer			
Benefit Information	N/A			
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory	Name, SSN identify patient for which assessments are being entered and reviewed.
Family Relation (spouse, children, parents, grandparents, etc)	No			
Service Information	Yes	Veteran	Mandatory	Service Connected for Spinal Cord Injury indicator for additional background on the nature of the injury; Active Military status to ascertain current occupational status

Medical Information

Diagnosis and treatment for injuries sustained with Spinal Cord Injury. Etiology/Date of Onset (nature of injury or disease and its onset); Ancillary Data Elements (historical treatment reference information); Brain Injury (whether additional complicating medical conditions exist); Other Injury (whether additional complicating medical conditions exist); First Seen in VA for SCI - (historical treatment reference)

Yes

Veteran

Mandatory

Criminal Record Information

No

Guardian Information

Education Information	Yes	Veteran	Mandatory	Highest level of education; hours spent working toward degree or in technical training - used to assess and direct rehabilitative or occupational therapies for the patient.
Benefit Information	Yes	Veteran	Mandatory	
Other (Explain) Age/ Sex/ Height/Weight	Yes	Veteran	Mandatory	Age/Sex/Height/Weight - used for clinical calculations, medical evaluation and decision support.
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		No			
Other Veteran Organization		No			
Other Federal Government Agency		No			
State Government Agency		No			
Local Government Agency		No			
Research Entity	Multiple VHA researchers make use of SCI data	Yes	Data sharing is limited to those items listed in the IRB approval for each research request. Items can include: SSN, level of injury, date of onset, assessment information, etc.	Both PII & PHI	Data steward working with the Office of Strategic Planning and Measurements reviews all research documentation for compliance with approvals (IRB and R&D), security training, etc before requesting permission from the SCI/D Chief Consultant to release data.
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system? Yes

Please enter the name of the system: VistA

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

5. Data Sharing & Access

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  
 Research       Sickle Cell       Other (Please Explain)

if yes, please check all that apply:

Describe process for authorizing access to this data.

Data steward reviews all research documentation for compliance with approval process before requesting permission from the SCI/D Chief Consultant to release data.

## (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: The design and development of the SCIDO application is strictly dictated by the contents of the Software Requirements Specification (SRS) document. The application itself presents strategically focused reviews of the clinically relevant data used to support the care and treatment of patients with spinal cord injuries and disorders.

How is data checked for completeness?

Answer: During field testing, data quality elements throughout the application are validated against the Legacy VistA/CPRS system for accuracy and completeness.

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

Answer: Diagnostic and procedural information is drawn from VistA in real time, while assessment information is documented directly into the regional database by SCI clinical and administrative staff.

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

Answer: The application displays clinical information filtered by programmatic constraints; one example is the Influenza Immunization report on the Medical Complications tab which presents diagnostic and procedural information for only influenza-related treatment and/or preventative care. Data outside the specified constraints are not displayed. Audit logs within the application can track assessment data directly to the end user for authentication and tracking purposes.

*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: Records will be maintained and disposed of in accordance with record disposition authority approved by the Archivist of the United States, 75 years after the death of the Veteran or after the date of last contact.

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

Answer: Records are retained in the event of a medical or legal review.

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

Answer: Depending on the record medium, records are destroyed by either shredding or degaussing. Optical disks or other electronic media are deleted when no longer required for official duties/purposes.

Where are these procedures documented?

Answer: Federal Register Volume 66, No. 103

How are data retention procedures enforced?

Answer: Archived paper records are labeled with a disposal date beyond which they can be shredded. Retention of electronic records is the responsibility of the System Owner.

---

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? No

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? No

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? No

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

Answer: The SCIDO application has not yet been fully deployed to the field. The application has built-in audits to track logins, registrations and assessments.

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

If 'No' please describe why:

Answer:

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

Answer: The project received FATO on 9/5/2008. Security scans were conducted by CyberSecurity staff at a representative SCI Center in Tampa, FL and at the Corporate Franchise Data Center in Austin, TX. Access to the application is base on roles, physically limiting access to SCIDO based on security key infrastructure. All users must sign User Access Agreements and Rules of Behavior and must complete Privacy and Security training annually. The SCIDO servers are installed in sanctioned computer rooms on VA campuses. Every VA computer room must have adequate physical security in place as documented in their Security Plan, The application has built-in audits to track logins, registrations, updates and assessments.

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 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 checked="" type="checkbox"/> Power Loss       |
| <input type="checkbox"/> Burglary/Break In/Robbery           | <input type="checkbox"/> Eavesdropping/Interception                       | <input type="checkbox"/> Sabotage/Terrorism          |
| <input type="checkbox"/> Cold/Frost/Snow                     | <input checked="" type="checkbox"/> Errors (Configuration and Data Entry) | <input type="checkbox"/> Storms/Hurricanes           |
| <input type="checkbox"/> Communications Loss                 | <input checked="" type="checkbox"/> Fire (False Alarm, Major, and Minor)  | <input type="checkbox"/> Substance Abuse             |
| <input type="checkbox"/> Computer Intrusion                  |   | <input type="checkbox"/> Theft of Assets             |

- Communications Loss
- Computer Intrusion
- Computer Misuse
- Data Destruction

- Fire (False Alarm, Major, and Minor)
- Flooding/Water Damage
- Fraud/Embezzlement

- Substance Abuse
- Theft of Assets
- Theft of Data
- Vandalism/Rioting

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. (Check all that apply)

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

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

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: None

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

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

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

The potential impact is **moderate** if the loss of confidentiality could be expected to have a serious 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 controls are being considered for the project based on the selections from the previous assessments?

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

---

*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.

Spinal Cord Injury and Disorders Outcomes (SCIDO) V 3.0 is a minor application running under Vista. There are no issues associated with this Minor Application that would supersede Vista.

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system? RAI/MDS

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

VBA Data Warehouse  
VBA Training Academy  
Veterans Canteen Web  
VIC  
VR&E Training Website  
Web LGY

Telecare Record Manager  
VBA Enterprise Messaging System  
Veterans On-Line Applications (VONAPP)  
Veterans Service Network (VETSNET)  
Web Electronic Lender Identification

Web Automated Folder Processing System (WAFPS)  
Web Automated Reference Material System (WARMS)  
Web Automated Verification of Enrollment  
Web-Enabled Approval Management System (WEAMS)  
Web Service Medical Records (WebSMR)  
Work Study Management System (WSMS)

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

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

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

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

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

ASISTS	Beneficiary Travel	Accounts Receivable	Adverse Reaction Tracking
Bed Control	Care Management	ADP Planning (PlanMan)	Authorization/ Subscription
CAPRI	Care Tracker	Bad Code Med Admin	Auto Replenishment/ Ward Stock
CMOP	Clinical Reminders	Clinical Case Registries	Automated Info Collection Sys
Dental	x CPT/ HCPCS Codes	Clinical Procedures	Automated Lab Instruments
x Dietetics	DRG Grouper	Consult/ Request Tracking	Automated Med Info Exchange
x 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
x 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
x Mailman	List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine	Mental Health	Generic Code Sheet	Interim Mangement Support
MICOM	MyHealthEVet	x Health Level Seven	x Master Patient Index VistA
NDBI	x National Drug File	Hospital Based Home Care	Missing Patient Reg (Original) A4EL
NOIS	Nursing Service	x Inpatient Medications	x Order Entry/ Results Reporting
Oncology	Occurrence Screen	Integrated Patient Funds	x PCE Patient Care Encounter
PAID	Patch Module	MCCR National Database	Pharmacy Benefits Mangement
x Prosthetics	Patient Feedback	Minimal Patient Dataset	Pharmacy Data Management
x QUASER	Police & Security	National Laboratory Test	Pharmacy National Database
x RPC Broker	Problem List	Network Health Exchange	Pharmacy Prescription Practice
SAGG	x Progress Notes	x Outpatient Pharmacy	Quality Assurance Integration
x Scheduling	Record Tracking	Patient Data Exchange	Quality Improvement Checklist
Social Work	x Registration	Patient Representative	x Radiology/ Nuclear Medicine
x 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	x Spinal Cord Dysfunction	CA Verified Components - DSSI
VBECs	x VistALink Security	x 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 &

RALS

VHA Enterprise Terminology  
Services

## (FY 2011) PIA: Final Signatures

Facility Name: CDCO>AITC>OI>VHIT> Spinal Cord Injury and Disorders

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

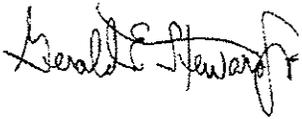
Privacy Officer:	Garnett Best	202-461-7474	Garnett.Best@va.gov
------------------	--------------	--------------	---------------------

Digital Signature Block

Information Security Officer:	Gerald Steward	210-616-8165	Gerald.Steward@va.gov
-------------------------------	----------------	--------------	-----------------------

5/17/2011

ture Block

X 

#REF!

#REF!

#REF!

Gerald Steward  
ISO

Digital Signature Block

Information Owner:	John F. Quinn	512-326-6188	John.Quinn@va.gov
--------------------	---------------	--------------	-------------------

Digital Signature Block

Other Titles: Program Manager	Larry J. Clark	202-245-1663	Larry.Clark2@va.gov
-------------------------------	----------------	--------------	---------------------

Digital Signature Block

Date of Report: 5/12/11

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

Project Name CDCO>AITC>OI>VHIT> Spinal Cord

Injury and Disorders

(FY 2011) PIA: Final Signatures

Facility Name: CDCO>AITC>OI>VHIT> Spinal Cord Injury and Disorders

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

Privacy Officer: Garnett Best 202-461-7474 Garnett.Best@va.gov

  
Digital Signature Block 7/7/2011

Information Security Officer: Gerald Steward 210-616-8165 Gerald.Steward@va.gov

Digital Signature Block

System Owner/ Chief Information Officer:

Digital Signature Block

Information Owner: John F. Quinn 512-326-6188 John.Quinn@va.gov



Other Titles: Program Manager Larry J. Clark 202-245-1663 Larry.Clark2@va.gov



Date of Report: 5/12/11

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

Project Name CDCO>AITC>OI>VHIT> Spinal Cord

Injury and Disorders