

## **Welcome to the PIA for FY 2010!**

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. More information can be found by reading VA 6508.

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 Privacy Impact Assessment Handbook 6202.2 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 Handbook 6202.2.
- 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 Handbook 6202.2 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

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 an individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirectly 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**

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.

## (FY 2010) PIA: System Identification

Program or System Name: Convergence Registries  
Development > AITC > Integrated Registries

OMB Unique System / Application / Program Identifier (AKA: UPID #): 104-05-01-006

The Convergence Registries system will be a single conceptual structure composed of multiple logical case-specific registries. The physical structure could be dispersed (and virtual) as the model is implemented and evolves. The dispersed structures could be either individual instances of registry-specific information or the repository of patient general clinical/demographic information.

Access to patient data within the registry is limited to those patients identified as belonging to a specific registry (Center of Excellence). Access controls are multi-layered and are specific to the assigned parameters and credentials of that individual user to allow "role-based" access. Patient-Registry inclusion indicators allow owners to access common demographics and clinical data, along with unique registry specific information. Clinical and demographics data is specific to the patient and independent of their inclusion in any registry. The application layer for each registry is independent of all registry functions but is unique to that registry. The filter functions for the data "extraction and update" interface are independent of the registry itself (and are unique to each data source).

### Description of System / Application / Program:

Facility Name: Austin Information Technology Center (AITC)

Title:	Name:	Phone:
Privacy Officer:	Amy Howe	512-326-6217
Information Security Officer:	Walter Whiteford	(512) 326-6294
Chief Information Officer:	Judy Downing	(512) 326-6000
Person Completing Document:	Rhonna Clark	(704) 681-2847
Other Titles:	Chuck Sternberg, Business Owner	(727) 319-1074

Other Titles:

Other Titles:

Date of Last PIA Approved by VACO Privacy

Services: (MM/YYYY) First PIA

Date Approval To Operate Expires: N/A

What specific legal authorities authorize this program or system: Title 38, United States Code, Section 501(b) and Section 304.

What is the expected number of individuals that will have their PII stored in this system: Potentially all Veterans

Identify what stage the System / Application / Program is at: Development/Acquisition

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. 04/2010

Is there an authorized change control process which documents any changes to existing applications or systems? N/A: First PIA

If No, please explain: PIA to be updated as minor applications are added. This is the first PIA.

Has a PIA been completed within the last three years? N/A: First PIA

Date of Report (MM/YYYY): 03/2010

**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 skip to TAB 12. ( See Comment for Definition of PII)**



Email:

[Amy.Howe1@va.gov](mailto:Amy.Howe1@va.gov)

[Walter.Whiteford@va.gov](mailto:Walter.Whiteford@va.gov)

[Judy.Downing@va.gov](mailto:Judy.Downing@va.gov)

[Rhonna.Clark@va.gov](mailto:Rhonna.Clark@va.gov)

[Charles.Sternberg2@va.gov](mailto:Charles.Sternberg2@va.gov)



Grey bar

Grey bar  
Yellow bar

Yellow bar

## (FY 2010) PIA: System of Records

---

Is the data maintained under one or more approved System(s) of Records?

Yes

if the answer above is no, please skip to row 16.

---

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

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

24VA19, 121VA19

2. Name of the System of Records:

Patient Medical Records-VA, National Patient  
Databases - VA,

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

[http://vaww.vhaco.va.gov/privacy/Update\\_SOR/SOR24VA19.pdf](http://vaww.vhaco.va.gov/privacy/Update_SOR/SOR24VA19.pdf)

---

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?

No

Is PII collected by verbal methods?

No

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 2010) 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)	VA File Database		Written	Written
Family Relation (spouse, children, parents, grandparents, etc)				
Service Information				
Medical Information	VA File Database		Written	Written
Criminal Record Information				
Guardian Information				
Education Information				
Benefit Information				
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	VA Files / Databases (Identify file)	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)				
Service Information				
Medical Information	Yes	VA Files / Databases (Identify file)	Voluntary	
Criminal Record Information				
Guardian Information				
Education Information				
Benefit Information				
Other (Explain)				
Other (Explain)				
Other (Explain)				

(FY 2010) 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	VHA	Yes	Care provider	Both PII & PHI	<a href="http://yaww.vhaco.va.gov/privacy/Update_SOR/SOR24VA19.pdf">http://yaww.vhaco.va.gov/privacy/Update_SOR/SOR24VA19.pdf</a>
Other Veteran Organization					
Other Federal Government Agency					
State Government Agency					
Local Government Agency					
Research Entity					
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2010) 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

Is there a contingency plan in place to process information when the system is down? Yes

(FY 2010) PIA: Secondary Use

Will PII data be included with any secondary use request? No

Drug/Alcohol Counseling     Mental Health     HIV

if yes, please check all that apply:  Research     Sickle Cell     Other (Please Explain)

Describe process for authorizing access to this data.

Answer:

**(FY 2010) 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: Responses are only provided to the questions applicable to the application.

How is data checked for completeness?

Answer: PIA is reviewed by individuals from the VA Privacy service

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

Answer: Annual review and maintenance of the PIA as required by policy.

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

Answer: PIA is reviewed by individuals from the VA Privacy service

*Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)*

Answer:

**(FY 2010) PIA: Retention & Disposal**

What is the data retention period?

Answer: Based on policy, 75 years upon death or last access of record (whichever is longer)

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

Answer: Based on regulatory requirements and VA policy.

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

Answer: VA Handbook 6500.1 Electronic Media Sanitization

Where are these procedures documented?

Answer: [http://vaww1.va.gov/vapubs/viewPublication.asp?Pub\\_ID=416&FType=2](http://vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=416&FType=2)

How are data retention procedures enforced?

Answer: Operating units and Information Security Officer supporting the application ensures standard operating procedures for media sanitization are followed according to policy requirements

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 2010) 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 2010) 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 Convergence Registries project has reviewed security requirements allocated by the Enterprise Requirement Management Te

---

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

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

Answer: (Other Risks)

---

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

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> Risk Management                                      | <input checked="" type="checkbox"/> Audit and Accountability          |
| <input checked="" type="checkbox"/> Access Control                                       | <input checked="" type="checkbox"/> Configuration Management          |
| <input checked="" type="checkbox"/> Awareness and Training                               | <input checked="" type="checkbox"/> Identification and Authentication |
| <input checked="" type="checkbox"/> Contingency Planning                                 | <input checked="" type="checkbox"/> Incident Response                 |
| <input checked="" type="checkbox"/> Physical and Environmental Protection                | <input checked="" type="checkbox"/> Media Protection                  |
| <input checked="" type="checkbox"/> Personnel Security                                   |   |
| <input checked="" type="checkbox"/> Certification and Accreditation Security Assessments |   |

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: System categorization is HIGH due to PHI/PII and VA sensitive data.

---

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 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.

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 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.

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 2010) PIA: Additional Comments**

---

Add any additional comments on this tab for any question in the form you want to comment on. Please indicate the question you are responding to and then add your comments.

---

There is no OMB number listed in the SMART database. The OMB number listed on Tab 2 reflects the OMB number for VistA AD - Application Development.

(FY 2010) PIA: VBA Minor Applications

Explain what minor application that are associated with your installation? *(Check all that apply)*

Records Locator System	Education Training Website	Appraisal System
Veterans Assistance Discharge System (VADS)	VR&E Training Website	Web Electronic Lender Identification
LGY Processing	VA Reserve Educational Assistance Program	CONDO PUD Builder
Loan Service and Claims	Web Automated Verification of Enrollment	Centralized Property Tracking System
LGY Home Loans	Right Now Web	Electronic Appraisal System
Search Participant Profile (SPP)	VA Online Certification of Enrollment (VA-ONCE)	Web LGY
Control of Veterans Records (COVERS)	Automated Folder Processing System (AFPS)	Access Manager
SHARE	Personal Computer Generated Letters (PCGL)	SAHSHA
Modern Awards Process Development (MAP-D)	Personnel Information Exchange System (PIES)	VBA Data Warehouse
Rating Board Automation 2000 (RBA2000)	Rating Board Automation 2000 (RBA2000)	Distribution of Operational Resources (DOOR)
State of Case/Supplemental (SOC/SSOC)	SHARE	Enterprise Wireless Messaging System (Blackberry)
Awards	State Benefits Reference System	VBA Enterprise Messaging System
Financial and Accounting System (FAS)	Training and Performance Support System (TPSS)	LGY Centralized Fax System
Eligibility Verification Report (EVR)	Veterans Appeals Control and Locator System (VACOLS)	Review of Quality (ROQ)
Automated Medical Information System (AMIS)290	Veterans On-Line Applications (VONAPP)	Automated Sales Reporting (ASR)
Web Automated Reference Material System (WARMS)	Automated Medical Information Exchange II (AIME II)	Electronic Card System (ECS)
Automated Standardized Performance Elements Nationwide (ASPEN)	Committee on Waivers and Compromises (COWC)	Electronic Payroll Deduction (EPD)
Inquiry Routing Information System (IRIS)	Common Security User Manager (CSUM)	Financial Management Information System (FMI)
National Silent Monitoring (NSM)	Compensation and Pension (C&P) Record Interchange (CAPRI)	Purchase Order Management System (POMS)
Web Service Medical Records (WebSMR)	Control of Veterans Records (COVERS)	Veterans Canteen Web
Systematic Technical Accuracy Review (STAR)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)	Inventory Management System (IMS)
Fiduciary STAR Case Review	Fiduciary Beneficiary System (FBS)	Synquest
Veterans Exam Request Info System (VERIS)	Hearing Officer Letters and Reports System (HOLAR)	RAI/MDS
Web Automated Folder Processing System (WAFPS)	Inforce	ASSISTS
Courseware Delivery System (CDS)	Awards	MUSE
Electronic Performance Support System (EPSS)	Actuarial	Bbraun (CP Hemo)
Veterans Service Representative (VSR) Advisor	Insurance Self Service	VIC
Loan Guaranty Training Website	Insurance Unclaimed Liabilities	BCMA Contingency Machines
C&P Training Website	Insurance Online	Script Pro

---

Baker System	Veterans Assistance Discharge System (VADS)
Dental Records Manager	VBA Training Academy
Sidexis	Veterans Service Network (VETSNET)
Priv Plus	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
Mental Health Assistant	BIRLS
Telecare Record Manager	Centralized Accounts Receivable System (CARS)
Omnicell	Compensation & Pension (C&P)
Powerscribe Dictation System	Corporate Database
EndoSoft	Control of Veterans Records (COVERS)
Compensation and Pension (C&P)	Data Warehouse
Montgomery GI Bill	INS - BIRLS
Vocational Rehabilitation & Employment (VR&E) CH 31	Mobilization
Post Vietnam Era educational Program (VEAP) CH 32	Master Veterans Record (MVR)
Spinal Bifida Program Ch 18	BDN Payment History
C&P Payment System	
Survivors and Dependents Education Assistance CH 35	
Reinstatement Entitlement Program for Survivors (REAPS)	
Educational Assistance for Members of the Selected Reserve Program CH 1606	
Reserve Educational Assistance Program CH 1607	
Compensation & Pension Training Website	
Web-Enabled Approval Management System (WEAMS)	
FOCAS	
Work Study Management System (WSMS)	
Benefits Delivery Network (BDN)	
Personnel and Accounting Integrated Data and Fee Basis (PAID)	
Personnel Information Exchange System (PIES)	
Rating Board Automation 2000 (RBA2000)	
SHARE	
Service Member Records Tracking System	

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.

Minor app #1	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?		

Minor app #2	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?		

Minor app #3	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 2010) PIA: VISTA Minor Applications

---

Explain what minor application that are associated with your installation? *(Check all that apply)*

ACCOUNTS RECEIVABLE	DRUG ACCOUNTABILITY	INPATIENT MEDICATIONS
ADP PLANNING (PLANMAN) ADVERSE REACTION TRACKING ASISTS	DSS EXTRACTS EDUCATION TRACKING EEO COMPLAINT TRACKING	INTAKE/OUTPUT INTEGRATED BILLING INTEGRATED PATIENT FUNDS
AUTHORIZATION/SUBSCRIPTION	ELECTRONIC SIGNATURE	INTERIM MANAGEMENT SUPPORT
AUTO REPLENISHMENT/WARD STOCK	ENGINEERING	KERNEL
AUTOMATED INFO COLLECTION SYS	ENROLLMENT APPLICATION SYSTEM	KIDS
AUTOMATED LAB INSTRUMENTS	EQUIPMENT/TURN-IN REQUEST	LAB SERVICE
AUTOMATED MED INFO EXCHANGE	EVENT CAPTURE	LETTERMAN
BAR CODE MED ADMIN	EVENT DRIVEN REPORTING	LEXICON UTILITY
BED CONTROL	EXTENSIBLE EDITOR	LIBRARY
BENEFICIARY TRAVEL	EXTERNAL PEER REVIEW	LIST MANAGER
CAPACITY MANAGEMENT - RUM	FEE BASIS	MAILMAN
CAPRI	FUNCTIONAL INDEPENDENCE	MASTER PATIENT INDEX VISTA
CAPACITY MANAGEMENT TOOLS	GEN. MED. REC. - GENERATOR	MCCR NATIONAL DATABASE
CARE MANAGEMENT CLINICAL CASE REGISTRIES	GEN. MED. REC. - I/O GEN. MED. REC. - VITALS	MEDICINE MENTAL HEALTH
CLINICAL INFO RESOURCE NETWORK	GENERIC CODE SHEET	MICOM
CLINICAL MONITORING SYSTEM	GRECC	MINIMAL PATIENT DATASET
CLINICAL PROCEDURES	HEALTH DATA & INFORMATICS	MYHEALTHVET
CLINICAL REMINDERS	HEALTH LEVEL SEVEN	Missing Patient Reg (Original) A4EL
CMOP	HEALTH SUMMARY	NATIONAL DRUG FILE
CONSULT/REQUEST TRACKING	HINQ	NATIONAL LABORATORY TEST
CONTROLLED SUBSTANCES	HOSPITAL BASED HOME CARE	NDBI
CPT/HCPCS CODES	ICR - IMMUNOLOGY CASE REGISTRY	NETWORK HEALTH EXCHANGE
CREDENTIALS TRACKING DENTAL DIETETICS	IFCAP IMAGING INCIDENT REPORTING	NOIS NURSING SERVICE OCCURRENCE SCREEN
DISCHARGE SUMMARY	INCOME VERIFICATION MATCH	ONCOLOGY
DRG GROUPER	INCOMPLETE RECORDS TRACKING	ORDER ENTRY/RESULTS REPORTING

---

OUTPATIENT PHARMACY	SOCIAL WORK
PAID PATCH MODULE PATIENT DATA EXCHANGE	SPINAL CORD DYSFUNCTION SURGERY SURVEY GENERATOR
PATIENT FEEDBACK	TEXT INTEGRATION UTILITIES
PATIENT REPRESENTATIVE	TOOLKIT
PCE PATIENT CARE ENCOUNTER PCE PATIENT/IHS SUBSET	UNWINDER UTILIZATION MANAGEMENT ROLLUP
PHARMACY BENEFITS MANAGEMENT PHARMACY DATA MANAGEMENT PHARMACY NATIONAL DATABASE PHARMACY PRESCRIPTION PRACTICE POLICE & SECURITY	UTILIZATION REVIEW VA CERTIFIED COMPONENTS - DSSI VA FILEMAN VBECs VDEF
PROBLEM LIST	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES	VHS&RA ADP TRACKING SYSTEM
PROSTHETICS QUALITY ASSURANCE INTEGRATION QUALITY IMPROVEMENT CHECKLIST QUASAR	VISIT TRACKING VISTALINK VISTALINK SECURITY VISUAL IMPAIRMENT SERVICE TEAM ANRV
RADIOLOGY/NUCLEAR MEDICINE RECORD TRACKING	VOLUNTARY TIMEKEEPING VOLUNTARY TIMEKEEPING NATIONAL
REGISTRATION	WOMEN'S HEALTH
RELEASE OF INFORMATION - DSSI	CARE TRACKER
REMOTE ORDER/ENTRY SYSTEM RPC BROKER	
RUN TIME LIBRARY SAGG SCHEDULING	
SECURITY SUITE UTILITY PACK	
SHIFT CHANGE HANDOFF TOOL	

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.

Minor app #1	Name		Description	Comments
		<input type="checkbox"/>	Is PII collected by this min or application?	
		<input type="checkbox"/>	Does this minor application store PII?	
			If yes, where?	
		Who has access to this data?		

Minor app #2	Name		Description	Comments
		<input type="checkbox"/>	Is PII collected by this min or application?	
		<input type="checkbox"/>	Does this minor application store PII?	
			If yes, where?	
		Who has access to this data?		

Minor app #3	Name		Description	Comments
		<input type="checkbox"/>	Is PII collected by this min or application?	
		<input type="checkbox"/>	Does this minor application store PII?	
			If yes, where?	
		Who has access to this data?		

(FY 2010) PIA: Minor Applications

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

Minor app #1	Name	Description	Comments
	Traumatic Brain Injury (TBI) Registry	<p>The TBI Registry will enhance the tracking of patients who may have experienced a traumatic brain injury. Review of the information collected also will allow VA to monitor quality of care and implement any identified improvements to the system of care. It would improve the VA's ability to analyze trends in health care needs and facilitate planning to meet TBI patient needs.</p> <p>The TBI Registry will be incorporated into a common database back-end and seamless front-end application structure, as part of the Registries Program Integration project. The Registries Database will be hosted on infrastructure within the Corporate Data Warehouse.</p>	
	<input checked="" type="checkbox"/> YES Is PII collected by this min or application?		
	<input checked="" type="checkbox"/> YES Does this minor application store PII?		
	If yes, where?		The TBI registry will be stored on the Convergence Registries system, on CDW in Austin, TX
Who has access to this data?		VA Providers	

Name	Description	Comments
Embedded Fragments Registry (EFR)	The Embedded Fragments	

Minor app #2		<p>Registry (EFR) will contain the names, contact information, medical history, bio-monitoring data and fragment information for all soldiers returning from the war with one or more embedded fragments. This information is needed to provide appropriate medical care and follow up monitoring for veterans with embedded fragments. The registry will be an integral part of the TEFSC, aiding in the development of medical and surgical treatment guidelines as well as enabling clinicians to deliver the most appropriate medical follow-up care to these veterans.</p> <p>The Global War On Terror (GWOT) report (recommendation P -7) prepared by the Presidential Task Force on Returning Global War on Terror Heroes states that the Department of Veterans Affairs (VA) shall create an Embedded</p>	
	<input checked="" type="checkbox"/>	Is PII collected by this min or application?	
	<input checked="" type="checkbox"/>	Does this minor application store PII?	
		If yes, where?	
		Who has access to this data?	VA Providers

Name	Description	Comments
Military/Veterans Eye Injury Registry (DVEIR)	<p>(*This project is also known as the DEFENSE AND VETERANS EYE INJURY REGISTRY(DVEIR))</p> <p>The VA-DoD Joint Eye Injury registry is required for ophthalmological and blind rehabilitation personnel of the Department of Defense and the Department of Veterans Affairs. This registry will be used to coordinate care, track longitudinal outcomes in order to facilitate research, and the development of best practices and clinical education, on eye injuries incurred by service members. Public Law 110-181 requires that data collected on service members sustaining significant eye injuries be shared bi-directionally between DoD and VA to ensure the coordination of the provision of ongoing eye care and visual rehabilitation benefits and services by the VA.</p> <p>Supports the DoDs Center of</p>	
	<input checked="" type="checkbox"/>	Is PII collected by this min or application?

YES	Does this minor application store PII?
	The DVEIR will be stored on the Convergence Registries system, on CDW in Austin, TX
	If yes, where?
	Who has access to this data?
	VA Providers, DoD Providers

## (FY 2010) PIA: Final Signatures

Facility Name: Austin Information Technology Center (AITC)

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

Privacy Officer:	Amy Howe	512-326-6217	Amy.Howe1@va.gov
------------------	----------	--------------	------------------

Digital Signature Block

Information Security Officer:	Walter Whiteford	(512) 326-6294	Walter.Whiteford@va.gov
-------------------------------	------------------	----------------	-------------------------

Digital Signature Block

Chief Information Officer:	Judy Downing	(512) 326-6000	Judy.Downing@va.gov
----------------------------	--------------	----------------	---------------------

Digital Signature Block

Person Completing Document:	Rhonna Clark	(704) 681-2847	Rhonna.Clark@va.gov
-----------------------------	--------------	----------------	---------------------

Digital Signature Block

System / Application / Program Manager:	Chuck Sternberg, Business Owner	(727) 319-1074	Charles.Sternberg2@va.gov
---	---------------------------------	----------------	---------------------------

Digital Signature Block

Date of Report: 3/1/2010  
OMB Unique Project Identifier: 104-05-01-006

Project Name

Convergence Registries  
Development > AITC > Integrated  
Registries