

Information		*Green Highlight = Must Answer Question		*Yellow Highlight = Required to Sign PIA	
Program or System Name:		Enrollment (aka EDB or IVM) [CDCO >AITC >VHA > HEC > Enrollment]			
OMB Unique System / Application / Program Identifier (AKA: UPID #):		029-00-01-11-01-1190-00			
Description of System/ Application/ Program : "must match what is stated in System Security Plan (SSP)"		<p>Enrollment Database - Income Verification Matching (EDB) is a central repository of veteran patient information residing at the Austin Information Technology Center (AITC) for the Veterans Health Administration (VHA) of the Department of Veteran Affairs. Social Security Administration (SSA) and Internal Revenue Service (IRS) data is included in this database and requires the appropriate security to prevent unauthorized disclosure of this information.</p> <p>EDB is a web-based application for the Health Eligibility Center (HEC) in Atlanta, Georgia. The Analysts at the HEC use the system to verify Veterans enrollment eligibility within the VHA healthcare system. The HEC performs a yearly Means Test on all Veterans whose eligibility is based on income. Each year analysts take the data reported by a Veteran and compare it to the information received from the IRS and SSA to determine an individual Veteran's eligibility. The Means Test results are reported back to the Veteran's VA Medical Center treating facility. EDB produces letter correspondence to assist the analysts in gathering information from the Veteran and also to inform the Veteran of any changes in their eligibility status.</p>			
Facility or Program Office Name:		Austin Information Technology Center (AITC)			
Title:		Name:		Phone:	
Privacy Officer:		Amy Howe		(512) 326-6217	
Information Security Officer:		Michael Francis		(404) 828-5319	
System Owner/Delegate:		John Rucker		(512) 326-6422	
Chief Information Officer:		John Rucker		(512) 326-6422	
Information Owner:		Tony Guagliardo		(404) 828-5300	
Other Titles:					
Person Completing Document:		Megan Edel		(512) 326-6890	
Other Titles:					
Date of Last Full Approved PIA by VACO Privacy Services: (MM/YYYY)		07/2008			
What specific legal authorities authorize this program or system:		Veterans' Health Care Eligibility Reform Act of 1996, Public Law 104-262; Title 38 U.S.C. Sections 1705, 1710, 1712 and 1722; Title 38 U.S.C Sections 5317 and 5319; Title 26 U.S.C. Section 6103 (I)(7)			
What is the expected number of individuals that will have their PII stored in this system:		10 million			
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.		9 years			
Is there an authorized change control process which documents any changes to existing applications or		<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PIA			
If No, (Explain on Tab 8)					

Is there a contingency plan in place to process information when the system is down?	<input checked="" type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A : First PIA
Has a PIA been completed within the last three years?	<input checked="" type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A : First PIA
FISMA QUESTIONS			
1. Is this a new system?	<input type="radio"/> Yes	<input checked="" type="radio"/> No	
2. Does this system contain Federal information in identifiable form?	<input checked="" type="radio"/> Yes	<input type="radio"/> No	
3. Does the system include information on the public?	<input checked="" type="radio"/> Yes	<input type="radio"/> No	
4. Is there a Privacy Impact Assessment (PIA) that covers this system?	<input checked="" type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> National Security System under 40 U.S.C. 11103, a PIA is not required for this system
5. Is Federal-owned information in this system retrieved by name or unique identifier?	<input checked="" type="radio"/> Yes	<input type="radio"/> No	
6. What is the System of Records Notice (SORN) for this system?	89VA16		
7. Has this SORN been reviewed or updated within the last three years?	Yes two years ago		
Date of Report (MM/YYYY):	1-Dec-11		
Any check mark in the boxes below will require a full PIA. Please continue to the next TAB and complete the remaining questions.			
If there is no Personally Identifiable Information on your system , please complete TAB 2 & TAB 12. (See Comment for Definition of PII)			
<input checked="" type="checkbox"/> Have any changes been made to the system since the last PIA?			
<input type="checkbox"/> Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?			
<input checked="" type="checkbox"/> Will this system/application/program retrieve information on the basis of name, unique identifier, symbol or other PII data?			
<input checked="" type="checkbox"/> Does this system/application/program collect, store, or disseminate PII/PHI data?			
<input checked="" type="checkbox"/> Does this system/application/program collect, store or disseminate the SSN?			

(FY 2012) PIA: System of Records

*Green Highlight = Must Answer Question

- 1. Is a SORN (System of Records Notice) Required?
- 2. Is there a SORN already in place?

<input checked="" type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> Not Sure
<input checked="" type="radio"/> Yes	<input type="radio"/> No	

***If Yes, select all of the appropriate SORN number(s):
 ***If Not Sure, continue to question 3

***Click to add. Delete SORN by highlighting SORN and comma if included and press the Delete key or place focus on area to delete all SORNs.

LIST OF SORN NUMBER(S) :

89VA16

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

- 3. If records are retrieved using any of the following entities, A SORN will be required (Please check all that apply)

<input checked="" type="checkbox"/> Full Name
<input checked="" type="checkbox"/> Maiden Name
<input type="checkbox"/> Mother's Maiden Name
<input type="checkbox"/> Alias
<input checked="" type="checkbox"/> Social Security Number
<input type="checkbox"/> Passport Number
<input type="checkbox"/> Driver's License Number
<input checked="" type="checkbox"/> Taxpayer Identification Number
<input type="checkbox"/> Financial Account Number
<input type="checkbox"/> Credit Card Number
<input checked="" type="checkbox"/> Street Address
<input checked="" type="checkbox"/> Email Address
<input type="checkbox"/> Photographic Image
<input type="checkbox"/> Fingerprints
<input type="checkbox"/> Handwriting
<input type="checkbox"/> Other Biometric Data
<input type="checkbox"/> Other (Explain on Tab 8)

- 4. Based on Question 3, is a SORN required?

<input checked="" type="radio"/> Yes	<input type="radio"/> No
<input checked="" type="radio"/> Yes	<input type="radio"/> No

***If Yes, has the process begun to obtain/acquire a SORN

Location where the specific applicable System of Records Notice may be accessed:

http://www.rms.oit.va.gov/SOR_Records.asp

(FY 2012) PIA: Data Collection And Storage ***Green Highlight = Must Answer Question**

Please fill in each column for the data types selected.				
Data Type	Collection Method	What are the subjects told about the intended use of their information?	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)	Paper	Eligibility	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	Paper	Eligibility	Written	Written
Service Information	Paper	Eligibility	Written	Written
Medical Information	Paper	Eligibility	Written	Written
Criminal Record Information	N/A			
Guardian Information	Paper	Eligibility	Written	Written
Education Information	N/A			
Benefit Information	VA File Database	Eligibility	Provided By Another System	Provided By Another System
Other (Explain on Tab 8)				
Data Type	Storage Method	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	<input checked="" type="radio"/> Yes <input type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Family Relation (spouse, children, parents, grandparents, etc)	<input checked="" type="radio"/> Yes <input type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Service Information	<input checked="" type="radio"/> Yes <input type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Medical Information	<input checked="" type="radio"/> Yes <input type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Criminal Record Information	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary	
Guardian Information	<input checked="" type="radio"/> Yes <input type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Education Information	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary	
Benefit Information	<input checked="" type="radio"/> Yes <input type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Other (Explain on Tab 8)	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary	
			(Please Select Yes/No)	
Proximity and Timing: Is the privacy notice provided at the time of data collection?			<input checked="" type="radio"/> Yes <input type="radio"/> No	
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?			<input checked="" type="radio"/> Yes <input type="radio"/> No	
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?			<input checked="" type="radio"/> Yes <input type="radio"/> No	
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?			<input checked="" type="radio"/> Yes <input type="radio"/> No	

(FY 2012) PIA: Data Sharing *Green Highlight = Must Answer Question		** Any connection external to VA requires an ISA/MOU per VA 6500. This section below must be consistent with your System Security Plan Interconnection Security Agreement section.			
Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VBA	<input checked="" type="radio"/> Yes <input type="radio"/> No	Patient Eligibility	<input checked="" type="radio"/> Yes <input type="radio"/> No	Internal
Other Veteran Organization	N/A	<input checked="" type="radio"/> Yes <input type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Other Federal Government Agency	IRS	<input type="radio"/> Yes <input checked="" type="radio"/> No	Income Verification	<input checked="" type="radio"/> Yes <input type="radio"/> No	Internal
Other Federal Government Agency	SSA	<input type="radio"/> Yes <input checked="" type="radio"/> No	Patient Eligibility	<input checked="" type="radio"/> Yes <input type="radio"/> No	Internal
State Government Agency	N/A	<input checked="" type="radio"/> Yes <input type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Local Government Agency	N/A	<input checked="" type="radio"/> Yes <input type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Research Entity		<input checked="" type="radio"/> Yes <input type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
<input checked="" type="checkbox"/> Other Project/ System (Explain on Tab 8)					
(FY 2012) PIA: Access to Records					
Does the system gather information from another system?		<input checked="" type="radio"/> Yes <input type="radio"/> No			
Please enter the name of the system:		HINQ, HEC Legacy (via VistA), ESR (via HEC Legacy)			
(FY 2012) PIA: Secondary Use					
Will PII data be included with any secondary use request?		<input type="radio"/> Yes <input checked="" type="radio"/> No			
Check all that apply		<input type="checkbox"/> Mental Health <input type="checkbox"/> HIV <input type="checkbox"/> Drug/Alcohol Counseling <input type="checkbox"/> Sickle Cell <input type="checkbox"/> Research <input type="checkbox"/> Other (Explain on Tab 8)			

(FY 2012) PIA: Records Management

*Green Highlight = Must Answer Question

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?

Yes (Explain on Tab 8) No

Is the data collected to only what is necessary to provide requested service?

Yes No (Explain on Tab 8)

Has the data provided been verified as complete?

Veteran Verified Received From Database Verification Unknown

(FY 2012) PIA: Retention & Disposal

What is the data retention period?

Paper records are destroyed after they have been accurately scanned on optical disks. Optical disks or other electronic medium are deleted when all phases of the veteran's appeal rights have ended (ten years after the income year for which the means test verification was conducted). Data received via Connect Direct to/from SSA and CD's/Tape from the IRS are destroyed 30 days after the data has been validated as being a good copy of the original data. Summary reports and other output reports are destroyed when no longer needed for current operation. Regardless of the record medium, no records are retired to a Federal records center.

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

Optical disks or other electronic medium are deleted when all phases of the veteran's appeal rights have ended (ten years after the income year for which the means test verification was conducted). Data received via Connect Direct to/from SSA and CD's/Tape from the IRS are destroyed 30 days after the data has been validated as being a good copy of the original data. Summary reports and other output reports are destroyed when no longer needed for current operation.

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

Depending on the record medium, records are destroyed by either shredding or degaussing.

Where are these procedures documented?

SORN 89VA16 - Income Verification Records.

How are data retention procedures enforced?

Data that is put into the database remains in the database forever. Data is not archived out to an external repository.

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

Yes No (Explain on Tab 8)

(FY 2012) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?

Yes (Explain on Tab 8) No

(FY 2012) PIA: Security *Green Highlight = Must Answer Question

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	<input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8)
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..	<input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8)
Is security monitoring conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	<input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8)
Is security assessment conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	<input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8)
Is adequate physical security in place to protect against unauthorized access?	<input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8)

*Ensure PE 2, PE-3, PE-6, PE-7, PE-8 have been addressed appropriately for your categorization

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

<input checked="" type="checkbox"/> Biological Release	<input checked="" type="checkbox"/> Fire	<input type="checkbox"/> Lightning Strike	<input type="checkbox"/> Terrorist
<input type="checkbox"/> Blizzard	<input type="checkbox"/> Flood	<input checked="" type="checkbox"/> Malicious Code	<input checked="" type="checkbox"/> Thunderstorm
<input type="checkbox"/> Burglary/Break In	<input checked="" type="checkbox"/> Hacker, Cracker	<input type="checkbox"/> Password Privacy Negligence	<input checked="" type="checkbox"/> Tornado
<input type="checkbox"/> Civil Unrest	<input type="checkbox"/> Hail	<input type="checkbox"/> Personnel Unavailable	<input type="checkbox"/> Tsunami
<input checked="" type="checkbox"/> Component Failure	<input checked="" type="checkbox"/> HAZMAT Release/Spill	<input checked="" type="checkbox"/> Power Failure	<input checked="" type="checkbox"/> User Negligence
<input type="checkbox"/> Dam Failure	<input checked="" type="checkbox"/> Human Health Emergency	<input type="checkbox"/> Sabotage	<input checked="" type="checkbox"/> User Sabotage
<input type="checkbox"/> Dust/Debris	<input type="checkbox"/> Hurricane	<input checked="" type="checkbox"/> System Intrusion, Break-Ins	<input type="checkbox"/> Vibration
<input type="checkbox"/> Earthquake	<input checked="" type="checkbox"/> HVAC Failure	<input checked="" type="checkbox"/> System Misconfiguration	<input type="checkbox"/> Volcano
<input type="checkbox"/> Extreme Cold	<input type="checkbox"/> Indoor Humidity	<input checked="" type="checkbox"/> System Penetration	<input type="checkbox"/> Water Damage
<input checked="" type="checkbox"/> Extreme Heat	<input type="checkbox"/> Landslide	<input checked="" type="checkbox"/> System Tampering	<input checked="" type="checkbox"/> Winter Weather Hazards

*If any other risks identified, explain in Tab 8

Based upon the risks identified above, Explain what security controls are being used to mitigate these risks. (Check all that apply)

<input checked="" type="checkbox"/> Access Control	<input checked="" type="checkbox"/> Configuration Management	<input checked="" type="checkbox"/> Media Protection	<input checked="" type="checkbox"/> System & Services Acquisition
<input checked="" type="checkbox"/> Audit & Accountability	<input checked="" type="checkbox"/> Contingency Planning	<input checked="" type="checkbox"/> Personnel Security	<input checked="" type="checkbox"/> System & Communication Protection
<input checked="" type="checkbox"/> Awareness & Training	<input checked="" type="checkbox"/> Identification & Authentication	<input checked="" type="checkbox"/> Physical & Environmental Protection	<input checked="" type="checkbox"/> System & Information Integrity
<input checked="" type="checkbox"/> Security Assessment & Authorization	<input checked="" type="checkbox"/> Incident Response	<input checked="" type="checkbox"/> Risk Assessment	<input checked="" type="checkbox"/> Planning <input checked="" type="checkbox"/> Maintenance

Answer: (Other Controls) Explain on Tab 8

PIA: PIA Assessment

Based upon NIST 800-60, volume II; List the Information data types chosen as a basis for your FIPS 199 System Categorization.

Answer:	
<p><u>Availability Assessment:</u> 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)</p>	<input type="checkbox"/> 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. <input checked="" type="checkbox"/> The potential impact is moderate if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> The potential impact is low if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
<p><u>Integrity Assessment:</u> If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? (Choose One)</p>	<input type="checkbox"/> 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. <input checked="" type="checkbox"/> The potential impact is moderate if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> The potential impact is low if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.
<p><u>Confidentiality Assessment:</u> If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? (Choose One)</p>	<input checked="" type="checkbox"/> 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. <input type="checkbox"/> The potential impact is moderate if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> 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.

(FY 2012) 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.

Basic demographic and eligibility data is shared with a number of VA systems since Enrollment data is essential information about the veteran. These systems include: Pharmacy (Outpatient/Inpatient Pharmacy and CMOP); Billing (Integrated Billing); PIMS (Patient Care Encounters, Event Capture, Scheduling, Ambulatory Care, Patient Transfer Facility program); Computerized Patient Record System; Ancillary Systems (Surgery, Lab, Radiology, Prosthetics); and CAPRI. All integration agreements (API and DBIA) are documented at the VHA level and submitted for approval according to VHA Standard Operation Procedures (SOPs). In addition, it is expected for all users of these systems to have signed security and confidentiality agreements prior to receiving access to each system (as per the VHA SOPs).

Demographic, eligibility, and enrollment data is also sent to VistA so that VA Medical Centers have the current information necessary to provide care to the veteran. As a result of the income verification process, this information often includes changes in eligibility for health care and the responsibility of the veteran to make co-payments for prior service received from facilities. Users at the medical centers must sign security and confidentiality agreements and receive security and privacy training prior to gaining access to VistA.

Core demographic, eligibility, financial assessment, and enrollment status information is sent to the National Enrollment Database (NED) via nightly messaging. The data is shared with NED to support national reporting requirements and to remove the reporting overhead from the HEC Legacy system. National enrollment reporting is a responsibility of the VHA Office of the Assistant Deputy Under Secretary for Health for Policy and Planning. The data received from the HEC Legacy system and stored in the NED resides on a DEC Alpha server that is on the AITC intranet. The standard AITC Security policies apply to anyone requesting or receiving access to the NED DEC Alpha server. Also, all users have taken the same security and privacy training that is required of all VA IT employees and contractors.

(FY 2012) PIA: VBA Minor Applications

Which of these are sub-components of your system?

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

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 2012) PIA: Minor Applications A-M

Which of these are sub-components of your system?

1184 Web	Clinical Info Resource Network		IFCAP
A4P	Clinical Monitoring System	Electronic Signature	Imaging
ACCu Care	Clinical Notes Templates	Embedded Fragment Registry	Incentive Awards
ACCU Check	Clinical Procedures	ENCORE 2	Incident Reporting
ACCU Med	Clinical Reminders	ENDSOFT	Income Verification Match
Adobe Acrobat	Clippership	Engineering	Incomplete Records Tracking
ADP Planning (PlanMan)	Combat Veteran Outreach	Enrollment Application System	Inpatient Medications
ADT	Committee on Waiver and Compromises		Intake/ Output
Adverse Reaction Tracking	Consult/ Request Tracking	Enterprise Terminology Server & VHA Enterprise Terminology Services	
Agent Cashier	Controlled Correspondence	ePROMISE	Integrated Billing
Air Fortress	Controlled Substances	Equipment/ Turn-in Request	Integrated Patient Funds
ASISTS	CP&E	Event Capture	Interim Mangement Support
Authorization/ Subscription	CPRS	Event Driven Reporting	Inventory Management System
Auto Instrument	CPT/ HCPCS Codes	Extensible Editor	Kernal
Auto Replenishment/ Ward Stock		External Peer Review	Kids
AUTOCAD	Credentials Tracking	EYECAP	KOWA
Automated Access Request	Credit Card Authentication	Fee Based Claims System	Lab Service
Automated Info Collection Sys	Data Innovations	Fee Basis	
Automated Lab Instruments	DELIVEREX	Financial and Accounting System (FAS)	
Automated Med Info Exchange	Dental	Financial Management System (FMS)	
Automated Sales Reporting	DICTATION-Power Scribe	Functional Independence	Laboratory Electronic Data Interchange
AutoMed	Dietetics	Gen. Med. Rec. - I/O	Letterman
Bad Code Med Admin	Discharge Summary	Gen. Med. Rec. - Vitals	Lexicon Utility
Barcode Medication Administration Contingency Plan (BCU)		Gen. Med.Rec. - Generator	Library
BCMA Contingency Workstations		GENDEX	List Manager
BDN 301	DRG Grouper	Generic Code Sheet	Lynx Duress Alarm
Beneficiary Travel	DRM Plus	Genesys	Mailman
Big Fix	Drug Accountability	Get Well Networks	MCCR National Database
CA Verified Components - DSSI		GMED	Meadows (MDWS)
Capacity Management - RUM	DSIT	GRECC	Medicine
Capacity Management Tools	DSS Extracts	Health Data and Informatics	Mental Health
CAPRI	DSS Quadramed	Health Level Seven	MHTP
Cardiff Teleform	EDS Whiteboard (AVJED)	Health Summary	MICOM
Cardiology Systems (stand alone servers from the network)		Health Summary Contingency	Microsoft Exchange E-mail System
Care Management	Education Tracking	HINQ	Military/Vet Eye Injury Registry
CareTracker	EEO Complaint Tracking	Hospital Based Home Care	Minimal Patient Dataset
CHECKPOINT	EKG System	ICB	Missing Patient Reg (Original) A4EL
Citrix	Electronic Card System (ECD)		Mumps AudioFAX
Clinical Case Registries	Electronic Payroll Deduction (EPD)		MyHealthEVet
Clinical Data Repository/Health Data Repository		ICR - Immunology Case Registry	

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 2012) PIA: Minor Applications N-Z

Which of these are sub-components of your system?

National Cemetery Association	Pharmacy Prescription Practice	Scheduling	VAMedSafe
National Drug File	PICIS OR	Security Suite Utility Pack	VBECS
National Laboratory Test	Police & Security	Sentillion	VDEF
NDBI	Problem List	Shift Change Handoff Tool	Vendor - Document Storage Sys
Network Health Exchange	Progress Notes	ShoreTel	Veterans Canteen Web
NOAHLINK	Prosthetics	Social Work	Veterans Information Solution
NOIS	Purchase Order Management System		VHAHUNAPP1
Nursing Service	Pyxis	Stellant	VHAHUNFPC1
Occurrence Screen	Q-Matic	Stentor	VHS & RA Tracking System
Omnicell	QMSI Prescription Processing	Surgery	Visit Tracking
Oncology	Quality Assurance Integration	Survey Generator	VISTA RAD
Onvicord (VLOG)	Quality Improvement Checklist	Telecare Record Manager	VISTA RO
Optifill	QUASER	Temp Trak	VistALink
Order Entry/ Results Reporting	Radiology/ Nuclear Medicine	Text Integration Utilities	VistALink Security
Outpatient Pharmacy	RAFT	Tickler Database	Visual Impairment Service Team ANRV
P2000 ROBOT	RALS	Toolkit	
PACS database	Record Tracking	TopCon	Vitria BusinessWare
Patch Module	Registration	TraceMaster	VIXS
Patient Data Exchange	Release of Information - DSSI	Tracking Continuing Education	
Patient Feedback	Remote Order/ Entry System	Traumatic Brain Injury	Voluntary Timekeeping
Patient Representative	RPC Broker	Unwinder	Voluntary Timekeeping National
PCE Patient Care Encounter	Run Time Library	Utility Management Rollup	WEB HINQ
Personal Computer Generated Letters		Utilization Review	Whiteboard
Pharmacy Benefits Mangement	SAGG	VA Conference Room Registration	
Pharmacy Data Management	SAN	VA Fileman	Women's Health
Pharmacy National Database	Scanning Exam and Evaluation System		Workload and Overtime

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?	

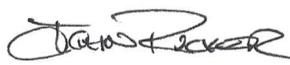
Name	
Description	
Comments	
Is PII collected by this minor application?	
Does this minor application store PII?	
If yes, where?	
Who has access to this data?	

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 2012) PIA: Final Signatures		*Green Highlight = Must Answer Question	
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:	Michael Francis	(404) 828-5319	Michael.Francis@va.gov
Digital Signature Block			
System Owner/Delegate:	John Rucker	(512) 326-6422	John.Rucker@va.gov
Digital Signature Block			
Chief Information Officer:	John Rucker	(512) 326-6422	John.Rucker@va.gov
Digital Signature Block			
Other Titles:	0	0	0
Digital Signature Block			
Date of Report:	1-Dec-11		
OMB Unique Project Identifier	029-00-01-11-01-1190-00		
Project Name	Enrollment (aka EDB or IVM) [CDCO >AITC >VHA> HEC > Enrollment]		

(FY 2012) PIA: Final Signatures

*Green Highlight = Must Answer Question

Facility Name:	0		
Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	512-326-6217	Amy.Howe1@va.gov
Digital Signature Block			
Information Security Officer:	0	0	0
Digital Signature Block			
System Owner/Delegate:	John Rucker	512-326-6422	John.Rucker@va.gov
Digital Signature Block 			
Chief Information Officer:	John Rucker	512-326-6422	John.Rucker@va.gov
Digital Signature Block 			
Other Titles:	0	0	0
Digital Signature Block			
Date of Report:	0-Jan-00		
OMB Unique Project Identifier	0		
Project Name	00000		