

(FY 2012) PIA: System Information		*Green Highlight = Must Answer Question		*Yellow Highlight = Required to Sign PIA	
Program or System Name (as shown in SMART):		CDCCO > AITC > VHA > CBO > PETIR - Portal for Electronic Third-party Insurance Recovery			
OMB Unique System / Application / Program Identifier (AKA: UPID #):		029-00-02-00-01-1120-00			
Description of System/ Application/ Program : "must match what is stated in System Security Plan (SSP)"		PETIR enables HIPAA-mandated electronic data exchanges between VAMC's VistA systems and health plans/payers (with the assistance of healthcare and financial clearinghouses, which are part of the HIPAA infrastructure). This national solution streamlines compliance with HIPAA by providing a single entity for managing the Electronic Data Interchange (EDI) IT infrastructure, processes and expertise. PETIR uses Commercial off-the Shelf (COTS) software to translate VistA data into HIPAA transaction formats, route the data to appropriate external trading partners, accept incoming transactions from external trading partners, and translate health plan statuses and responses into formats acceptable to VistA before returning the information to VistA.			
Facility or Program Office Name:		Austin Information Technology Center (AITC)			
Title:		Name:		Phone:	
Privacy Officer:		Amy Howe		512-326-6217	
Information Security Officer:		Leigh Taylor		512-460-5321	
System Owner/Delegate:		John Rucker		512-326-6422	
Chief Information Officer:		John Rucker		512-326-6422	
Information Owner:					
Other Titles:					
Person Completing Document:		Analida Aguilar		512-326-6042	
Other Titles:					
Date of Last Full Approved PIA by VACO Privacy Services: (MM/YYYY)				06/2009	
What specific legal authorities authorize this program or system:		Title 38, United States Code, sections 1710 and 1729.			
What is the expected number of individuals that will have their PII stored in this system:		Approximately 900,000			
Identify what stage the System / Application / Program is at:		Operations/Maintenance			
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.		7 years			
Is there an authorized change control process which documents any changes to existing applications or systems?		<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?		114VA16, 79VA19			
7. Has this SORN been reviewed or updated within the last three years?		Yes two years ago			
Date of Report (MM/YYYY):		8-Nov-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 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?				
Directions				

(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) :

114VA16, 79VA19

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 checked="" 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 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)	Electronic/File Transfer	Healthcare	Provided By Another System	Provided By Another System
Family Relation (spouse, children, parents, grandparents, etc)	Electronic/File Transfer	Healthcare	Provided By Another System	Provided By Another System
Service Information	N/A	N/A	N/A	N/A
Medical Information	Electronic/File Transfer	Healthcare	Provided By Another System	Provided By Another System
Criminal Record Information	N/A	N/A	N/A	N/A
Guardian Information	Electronic/File Transfer	Healthcare	Provided By Another System	Provided By Another System
Education Information	N/A	N/A	N/A	N/A
Benefit Information	N/A	N/A	N/A	N/A
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	VA Files/Databases (VistA)	<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	Automated
Family Relation (spouse, children, parents, grandparents, etc)	<input checked="" type="radio"/> Yes <input type="radio"/> No	VA Files/Databases (VistA)	<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	Automated
Service Information	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Medical Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	VA Files/Databases (VistA)	<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	Automated
Criminal Record Information	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Guardian Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	VA Files/Databases (VistA)	<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	Automated
Education Information	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Benefit Information	<input type="radio"/> Yes <input checked="" 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 checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
	<i>(Please Select Yes/No)</i>			
Proximity and Timing: Is the privacy notice provided at the time of data collection?	<input type="radio"/> Yes <input checked="" type="radio"/> No			
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	<input type="radio"/> Yes <input checked="" type="radio"/> No			
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	<input type="radio"/> Yes <input checked="" type="radio"/> No			
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	<input type="radio"/> Yes <input checked="" type="radio"/> No			
	routine use(s)			

(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	VHA	<input checked="" type="radio"/> Yes <input type="radio"/> No	Insurance	<input checked="" type="radio"/> Yes <input type="radio"/> No	HIPAA Authorization/Waiver
Other Veteran Organization		<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Other Federal Government Agency	Health and Human Services (HHS), Centers for Medicare and Medical Services (CMS) via CMS-contracted Fiscal Intermediary, TrailBlazer Health Enterprises	<input type="radio"/> Yes <input checked="" type="radio"/> No	Insurance	<input checked="" type="radio"/> Yes <input type="radio"/> No	HIPAA Authorization/Waiver
State Government Agency		<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Local Government Agency		<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Research Entity		<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
<input checked="" type="checkbox"/> Other Project/ System (Explain on Tab 8)	Health plans/agents, Emdeon-Envoy LLC, VisionShare, MedData and PNC Bank	No	Insurance - These entities are part of the healthcare industry's network infrastructure supporting HIPAA-mandated data exchanges.	Yes PII & PHI	HIPAA Authorization/Waiver
(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:		VHA Vista system and health plans/clearinghouses (through Emdeon, VisionShare, MedData, and PNC Bank).			
(FY 2012) PIA: Secondary Use					
Will PII data be included with any secondary use request?		<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="checkbox"/> Mental Health	<input type="checkbox"/> HIV	<input type="checkbox"/> Drug/Alcohol Counseling
Check all that apply		<input type="checkbox"/> Sickle Cell	<input type="checkbox"/> Other (Explain on Tab 8)		<input type="checkbox"/> Research

(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?			
<input type="radio"/> Yes (Explain on Tab 8)		<input checked="" type="radio"/> No	
Is the data collected to only what is necessary to provide requested service?			
<input checked="" type="radio"/> Yes		<input type="radio"/> No (Explain on Tab 8)	
Has the data provided been verified as complete?			
<input type="checkbox"/> Veteran Verified		<input checked="" type="checkbox"/> Received From Database	
		<input type="checkbox"/> Verification Unknown	
(FY 2012) PIA: Retention & Disposal			
What is the data retention period?		RCS 10-1 link for VHA: www.va.gov/vhapublications/rcs10/rcs10-1.pdf	
Retention period is seven (7) years for each electronic data transaction.		RCS VB-1, Part II Revised for VBA: www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/part2.pdf	
		National Archives and Records Administration: www.nara.gov	
Explain why the information is needed for the indicated retention period?			
Answer: Retention period for HIPAA transactions specified by the Department of Health and Human Services (HHS) Centers for Medicare and Medicaid Services (CMS).			
What are the procedures for eliminating data at the end of the retention period?			
Answer: At the end of the retention period data is automatically archived.			
Where are these procedures documented?			
Answer: These procedures are documented in the system design document.			
How are data retention procedures enforced?			
Answer: Data retention procedures are enforced via audit requirements established by the System Owner.			
Has the retention schedule been approved by the National Archives and Records Administration (NARA)?			
<input checked="" type="radio"/> Yes		<input type="radio"/> 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?			
<input type="radio"/> Yes (Explain on Tab 8)		<input checked="" type="radio"/> 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. Yes 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. Yes No (Explain on Tab 8)

Is security monitoring conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information? Yes No (Explain on Tab 8)

Is security assessment conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information? Yes No (Explain on Tab 8)

Is adequate physical security in place to protect against unauthorized access? Yes 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 type="checkbox"/> Biological Release	<input type="checkbox"/> Fire	<input type="checkbox"/> Lightning Strike	<input type="checkbox"/> Terrorist
<input type="checkbox"/> Blizzard	<input type="checkbox"/> Flood	<input type="checkbox"/> Malicious Code	<input type="checkbox"/> Thunderstorm
<input type="checkbox"/> Burglary/Break-In	<input type="checkbox"/> Hacker, Cracker	<input type="checkbox"/> Password Privacy Negligence	<input 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 type="checkbox"/> HAZMAT Release/Spill	<input type="checkbox"/> Power Failure	<input type="checkbox"/> User Negligence
<input type="checkbox"/> Dam Failure	<input type="checkbox"/> Human Health Emergency	<input type="checkbox"/> Sabotage	<input type="checkbox"/> User Sabotage
<input type="checkbox"/> Dust/Debris	<input type="checkbox"/> Hurricane	<input checked="" type="checkbox"/> System Intrusion/Break-In	<input type="checkbox"/> Vibration
<input type="checkbox"/> Earthquake	<input type="checkbox"/> IcyAC Failure	<input checked="" type="checkbox"/> System Misconfiguration	<input type="checkbox"/> Yellows
<input type="checkbox"/> Extreme Cold	<input type="checkbox"/> Indoor Humidity	<input type="checkbox"/> System Penetration	<input type="checkbox"/> Water Damage
<input type="checkbox"/> Extreme Heat	<input type="checkbox"/> Landslide	<input type="checkbox"/> System Tempering	<input 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 and Services Acquisition
<input checked="" type="checkbox"/> Audit and Accountability	<input checked="" type="checkbox"/> Contingency Planning	<input checked="" type="checkbox"/> Personnel Security	<input checked="" type="checkbox"/> System and Communication Protection
<input checked="" type="checkbox"/> Awareness and Training	<input checked="" type="checkbox"/> Identification and Authentication	<input checked="" type="checkbox"/> Physical and Environmental Protection	<input checked="" type="checkbox"/> System and Information Integrity
<input checked="" type="checkbox"/> Security Assessment and 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 FIS 199 System Categorization.

Answer:

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

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

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

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

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

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

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

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

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

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

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

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

The controls are being considered for the project based on the selections from the previous assessments? The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; 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.

The PETIR initiative is sponsored by the VHA Chief Business Office, developed by the Financial Services Center (FSC) and hosted at the AITC. PETIR serves as the HIPAA-gateway between VAMC VistA systems and healthcare clearinghouses/health plans and includes the following capabilities:

EDM - 1) translates VistA files into the HIPAA-compliant formats for Request for Medicare-equivalent Remittance Advice (**eMRA**), Third-party Health Care Claims (**eClaims**) and transmits them to healthcare clearinghouses/health plans and 2) accepts healthcare clearinghouse/health plan responses and Third-party Claims Payments (**ePayments**) and translates them into VistA-acceptable formats and returns them to VistA.

EPH - is the ePayments database containing copies of the payment and explanation of benefit information. The database allows FSC 224 Section staff to reconcile unroutable information and direct the information to the appropriate VAMC.

IIV - 1) translates VistA files into the HIPAA-compliant request for Insurance Verification (**eIV**) and transmits them to healthcare clearinghouses/health plans and 2) accepts healthcare clearinghouse/health plan responses and translates them into VistA-acceptable format and returns them to VistA .

PHR - 1) translates VistA files into the HIPAA-compliant Pharmacy Claims (**ePharmacy**) and transmits them to healthcare clearinghouses/health plans and 2) accepts healthcare clearinghouses/health plan responses and translates them into VistA-acceptable format and returns them to VistA.

ETA - EDI Transaction Management/Analysis Tool (Edifecs) is a software suite that is used by the FSC to perform analysis and reporting on electronic medical claims and insurance verification transactions.

Tab 4 notes: VAMC staff collect then enter the data into the VHA VistA systems, and provide all privacy notices. Data is then electronically transmitted to PETIR for execution of HIPAA-mandated electronic data exchanges.

Tab 5 notes: VHA VAMC/health plan data exchanges use Emdeon, MedData (healthcare clearinghouses), PNC Bank (Treasury-designated electronic healthcare lockbox bank) & VisionShare (Medicare connection service) as connection points between PETIR and health plans. They are part of the healthcare industry's network infrastructure supporting HIPAA-mandated data exchanges.

(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		Automated Medical Information System (AMIS)290
Appraisal System	Centralized Property Tracking System	Automated Standardized Performance Elements Nationwide (ASPEN)
ASSISTS	Common Security User Manager (CSUM)	Broome Closet
Awards	Compensation and Pension (C&P)	Centralized Accounts Receivable System (CARS)
Baker System	Control of Veterans Records (COVERS)	Committee on Waivers and Compromises (COWC)
Bbraun (CP Hemo)	Courseware Delivery System (CDS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
	Dental Records Manager	
	Education Training Website	Compensation & Pension Training Website
C&P Payment System	Electronic Appraisal System	Distribution of Operational Resources (DOOR)
C&P Training Website	Electronic Card System (ECS)	Educational Assistance for Members of the Selected Reserve Program CH 1606
CONDO PUD Bullder	Electronic Payroll Deduction (EPD)	Electronic Performance Support System (EPSS)
	Eligibility Verification Report (EVR)	Enterprise Wireless Messaging System (Blackberry)
	Fiduciary Beneficiary System (FBS)	Financial Management Information System (FMII)
	Fiduciary STAR Case Review	Hearing Officer Letters and Reports System (HOLAR)
EndoSoft	Financial and Accounting System (FAS)	Inquiry Routing Information System (IRIS)
FOCAS	Insurance Unclaimed Liabilities	
Inforce	Inventory Management System (IMS)	Modern Awards Process Development (MAP-D)
INS - BIRLS	Interactive Voce Response (IVR)	Personal Computer Generated Letters (PCGL)
Insurance Online	LGV Centralized Fax System	Personnel Information Exchange System (PIES)
Insurance Self Service	Loan Service and Claims	Post Vietnam Era educational Program (VEAP) CH 32
LGY Home Loans	Loan Guaranty Training Website	Purchase Order Management System (POMS)
LGY Processing		Reinstatement Entitlement Program for Survivors (REAPS)
MES	Mental Health Assistant	Reserve Educational Assistance Program CH 1607
Mobilization	National Silent Monitoring (NSM)	RightFax
Montgomery GI Bill	Powerscribe Dictation System	Service Member Records Tracking System
MUSE	Rating Board Automation 2000 (RBA2000)	Survivors and Dependents Education Assistance CH 35
Omnicell	Records Locator System	Systematic Technical Accuracy Review (STAR)
Priv Plus	Remittance Processing System	Training and Performance Support System (TPSS)
RAI/MDS	Review of Quality (ROQ)	VA Online Certification of Enrollment (VA-ONCE)
Right Now Web	Search Participant Profile (SPP)	VA Reserve Educational Assistance Program
SAHSHA	Spinal Bifida Program Ch 18	
Script Pro	State Benefits Reference System	Veterans Assistance Discharge System (VADS)
SHARE	State of Case/Supplemental (SOC/SSOC)	Veterans Exam Request Info System (VERIS)
Sidexis	Telecare Record Manager	Veterans Insurance Claims Tracking and Response System (VICTARS)
Synquest	VBA Enterprise Messaging System	Veterans Service Representative (VSR) Advisor
VBA Training Academy		Vocational Rehabilitation & Employment (VR&E) CH 31
Veterans Canteen Web	Web Electronic Lender Identification	Web Automated Folder Processing System (WAFPS)
VETSNET Housekeeping		Web Automated Reference Material System (WARMs)
VR&E Training Website		Web Automated Verification of Enrollment
Web LGY		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 2012) PIA: Minor Applications A-M

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

Which of these are sub-components of your system?			
National Cemetery Association	Pharmacy Data Management	Scanning Exam and Evaluation System	VBECs
National Drug File	Pharmacy National Database	Scheduling	VDEF
National Laboratory Test	Pharmacy Prescription Practice	Security Suite Utility Pack	Vendor - Document Storage Sys
NDBI	PICIS OR	Sentillion	Veterans Canteen Web
Network Health Exchange	Police & Security	Shift Change Handoff Tool	Veterans Information Solution
NOAHLINK	Problem List	ShoreTel	VHAHUNAPP1
NOIS	Progress Notes	Social Work	VHAHUNFPC1
Nursing Service	Prosthetics	Stellant	VHS & RA Tracking System
Occurrence Screen	Purchase Order Management System	Stentor	Visit Tracking
Omniceil	Pyxis	Surgery	VISTA RAD
Oncology	Q-Matic	Survey Generator	VISTA RO
Onvicord (VLOG)	QMSI Prescription Processing	Telecare Record Manager	VistALink
Optifill	Quality Assurance Integration	Temp Trak	VistALink Security
Order Entry/ Results Reporting	Quality Improvement Checklist	Text Integration Utilities	Visual Impairment Service Team ANRV
Outpatient Pharmacy	QUASER	Tickler Database	Vitra BusinessWare
P2000 ROBOT	Radiology/ Nuclear Medicine	Toolkit	VIXS
PACS database	RAFT	TopCon	Voluntary Timekeeping
Patch Module	RALS	TraceMaster	Voluntary Timekeeping National
Patient Data Exchange	Record Tracking	Tracking Continuing Education	WEB HINQ
Patient Feedback	Registration	Traumatic Brain Injury	Whiteboard
Patient Representative	Release of Information - DSSI	Unwinder	Women's Health
PCE Patient Care Encounter	Remote Order/ Entry System	Utility Management Rollup	Workload and Overtime
Personal Computer Generated Letters	RPC Broker	Utilization Review	
Pharmacy Benefits Mangement	Run Time Library	VA Conference Room Registration	
	SAGG	VA Fileman	
	SAN	VAMedSafe	
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:	Leigh Taylor	512-460-5321	leigh.taylor@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:	8-Nov-11		
OMB Unique Project Identifier	029-00-02-00-01-1120-00		
Project Name	CDCO > AITC > VHA > CBO > PETIR - Portal for Electronic Third-party Insurance Recovery		
<p>The Signature Process:</p> <ul style="list-style-type: none"> • Complete the PIA form. • Name the PIA Excel FORM ["FY12-Region # - Facility Name - Facility # -Date(mmddyyyy).xls"] <ul style="list-style-type: none"> • Example: "FY12-Region3-Lexington VAMC-596-10302008.xls" • Submit the completed PIA Excel form to SMART Database. • Fix errors the reviewers sent back, rename the file and submit to SMART Database <ul style="list-style-type: none"> • If no errors, convert form into PDF with Nuance PDF Professional. • Name the PIA PDF form ["FY12-Region #-Facility Name- Facility # -Date(mmddyyyy).xls"] <ul style="list-style-type: none"> • Obtain digital signatures on the "Final Signatures tab" • Submit signed PIA PDF form to the SMART Database. 			

(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:	Leigh Taylor	0	0 0
Digital Signature Block <i>Leigh Taylor</i>			
System Owner/Delegate:	John Rucker	512-326-6422	John.Rucker@va.gov
Digital Signature Block <i>John Rucker</i>			
Chief Information Officer:	John Rucker	512-326-6422	John.Rucker@va.gov
Digital Signature Block <i>John Rucker</i>			
Other Titles:	0	0 0	
Digital Signature Block			
Date of Report:	0-Jan-00		
OMB Unique Project Identifier	0		
Project Name	00000		