

Welcome to the PIA for FY 2011!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vawww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 referenced in the procedure section of this document.

- a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Directive 6508.
- b. Records Officer is responsible for supplying records retention and deletion schedules.
- c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Directive 6508 and to immediately report all anomalies to the Privacy Service and appropriate management chain.
- d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.
- e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

Microsoft Office 2003: To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

Microsoft Office 2007: To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable

All Macros; 2) Click OK

Final Signatures

Final Signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.

Privacy Impact Assessment Uploaded into SMART

Privacy Impact Assessments should be uploaded into C&A section of SMART.

All PIA Validation Letters should be emailed to christina.pettit@va.gov to received full credit for submission.

(FY 2011) PIA: System Identification

Program or System Name: CDCO > AITC > VHA > My HealtheVet
 OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-01-11-01-1242-00
 Description of System/ Application/ Program: My HealtheVet is a free, online Personal Health Record that allows Veterans to record, track and store important health and military history information at their convenience.

Facility Name: CDCO AITC

Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	(512) 326-6217	Amy.Howe1@va.gov
Information Security Officer:	Paula Pinckney	(301) 734-0438	Paula.Pinckney@va.gov
System Owner/ Chief Information Officer:	John Rucker	(512) 326-6000	John.Rucker@va.gov
OI&T OED Project Manager	Patricia Simon	(315) 587-6014	Patricia.Simon2@va.gov
Information Owner (VHA)	Theresa Hancock	(301) 734-0371	Theresa.Hancock@va.gov
Business Owner	Madhulika Agarwal	(202) 461-7590	Madhulika.Agarwal.va.gov
Other Titles: AITC Project Manager	James Magness	(512) 326-6282	James.Magness@va.gov
Person Completing Document:	Megan Edel	(512) 326-6890	Megan.Edel@va.gov

Other Titles:
 Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY) 06/2009
 Date Approval To Operate Expires: 08/2011

What specific legal authorities authorize this program or system: Title 38, United States Code, Section 501
 What is the expected number of individuals that will have their PII stored in this system: 100,000-999,999
 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? Yes
 If No, please explain:
 Has a PIA been completed within the last three years? Yes
 Date of Report (MM/YYYY): 11/2010

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/DHI data?
- Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system, please complete TAB 7 & TAB 12. (See Comment for Definition of PII)

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.

Yes

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

- | | |
|---|---|
| 1. All System of Record Identifier(s) (number): | My HealtheVet Administrative Records-VA (130VA19) |
| 2. Name of the System of Records: | My HealtheVet Administrative Records-VA
(Under amendment) |
| 3. Location where the specific applicable System of Records Notice may be accessed (include the URL): | http://www.federalregister.gov/articles/2010/11/17/2010-28950/privacy-act-of-1974-system-of-records#p-9 |

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

Yes

Does the System of Records Notice require modification or updating?

No

(Please Select Yes/No)

Is PII collected by paper methods?

Yes

Is PII collected by verbal methods?

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 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Web form	The information is for MHV use only and is stated in the Privacy Notice.	Automated	Automated
Family Relation (spouse, children, parents, grandparents, etc)	Web form	For emergency contact and health history.	Automated	Automated
Service Information	Web form	Voluntary by the veteran - self entered. Allows them to share with others.	Automated	Automated
Medical Information	Web form	Voluntary by the veteran - self entered. Allows them to share with others. Patients use the information to coordinate their care. Includes medications (voluntary and VistA electronic record) and allows them to reorder.	Automated	Automated
Criminal Record Information				
Guardian Information				
Education Information				
Benefit Information				
Other (Explain)				
Delegation information	Web form	Forthcoming - user (Veteran) delegates who can access their information.	Automated	Automated

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	
Service Information	Yes	VA Files / Databases (Identify file)	Voluntary	VistA and Veteran
Medical Information	Yes	VA Files / Databases (Identify file)	Voluntary	VistA and Veteran
Criminal Record Information	No			
Guardian Information	No			
Education Information	No			
Benefit Information	No			
Other (Explain) - Delegation info Other (Explain) Other (Explain)	Yes	Veteran	Voluntary	Veteran

(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	N/A				
Other Veteran Organization	N/A				
Other Federal Government Agency	N/A				
State Government Agency	N/A				
Local Government Agency	N/A				
Research Entity	N/A				
Other Project / System	N/A				
Other Project / System	N/A				
Other Project / System	N/A				

(FY 2011) PIA: Access to Records

Does the system gather information from another system? Yes

Please enter the name of the system: Master Patient Index/ 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 2011) PIA: Secondary Use

Will PII data be included with any secondary use request? Yes

if yes, please check all that apply:

- Drug/Alcohol Counseling
- Mental Health
- HIV
- Research
- Sickle Cell
- Other (Please Explain)

Describe process for authorizing access to this data.

Answer: Mental Health information is available as part of the My Recovery. Users must agree to delegation of that information to Clinical Team. Data Use Agreement must be completed by requestor and approved by the system manager of record.

(FY 2011) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: Veterans own their own data; the VA is the middleman. Any information entered by the Veteran is voluntary.

How is data checked for completeness?

Answer: Required fields during registration perform error checking. Voluntary data entered by Veterans isn't checked.

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

Answer: Self-entered information is maintained by Veterans. Medical records are polled at the request of veterans; otherwise, it is updated every day at midnight.

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

Answer: Self-entered information isn't verified. Data placed by the VA comes from the electronic medical record which was validated by VistA and CPRS. Wellness reminders go through a translation tables.

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

Answer:

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: The Veterans self-entered record is to be maintained indefinitely.

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

Answer: The information belongs to the veteran and is longitudinal (birth to after death).

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

Answer: No data is eliminated.

Where are these procedures documented?

Answer: There are no procedures for data disposal.

How are data retention procedures enforced?

Answer: Data retention is to keep it indefinitely. To keep the data, it is archived.

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

Yes

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

Answer:

(FY 2011) PIA: Children's Online Privacy Protection Act (COPPA)

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

No

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 2011) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured. Yes

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.. Yes

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? 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: Prior to production, a C&A with the ATO was completed. Prior to receiving access, user completed and signed User Access Request Forms. The user acknowledged and signed he/she would abide by the Rules of Behavior. The user also completed mandatory security and privacy awareness training.

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

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

Answer: (Other Risks)

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

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

Answer: (Other controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer: None.

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

- The potential impact is **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; 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 2011) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question.

My Health e Vet (MHV) is a web-based personal health record system that provides Veterans with information and tools that they can use to increase their knowledge about health conditions, increase communication with their care providers and improve their own health. Level one Veterans (who have a MHV account hosted behind the VA firewall which follows VA approved guidelines for user name and strong password) are able to access health education tools and resources, create and maintain a secure comprehensive personal health record, and request VA prescription refills online. Authenticated level two Veterans are able to receive electronic copies of their health information, view VA wellness reminders, communicate with their providers through secure messaging, and access a number of other functions and options related to their health maintenance and health information. VA also provides, through a web-based environment, a secure and private health space where Veterans can enter their own personal and medical information in a "self-entered" health information section.

Electronic copies of health information are not considered VA authoritative records, nor are they considered part of the VA system of records once they are downloaded into the Veteran's secure and private health space. The Veteran's self-entered health information is also owned and maintained by the Veteran in the My Health e Vet secure and private health space and is not by itself a part of the VA's system of records. This self-entered health information may be included in the Veteran's official VA electronic health record upon the Veteran's request and/or upon VA's determination that it is appropriate to include it in the official medical record.

Certain applications of My Health e Vet may generate or result in data and information that is included in another VA system of records, such as secure messages which are generated from the My Health e Vet application but are included in 24VA19 system of records due to the potential for clinically relevant information to be contained within a secure message. Administrative data associated with such applications will be included in the My Health e Vet Administrative Records—VA system of records. Show citation box

Certain applications of My Health e Vet may interface with other VA maintained programs or applications to allow communication from the Veteran to the specific application or program, such as eBenefits applications, a VA/DoD joint portal. Certain administrative data may be maintained by My Health e Vet as a result of these applications or exchanges; however, the VA maintained program or application receiving the information will maintain the authoritative information of record.

My Health e Vet may also be used, upon permission from the Veteran, as a Health Information Exchange point, between a VA approved agency or organization and the Veteran's personal health record.

VA does not provide access to the Veteran's personal health information maintained in My Health e Vet in any situation, including medical emergency situations. If a non-VA health care provider requires information from VA medical records to treat a Veteran patient, the non-VA health care provider must obtain the Veteran's consent to release information and contact the VA facility where the Veteran patient was last treated to obtain information.

Delegation of My Health e Vet will allow Veterans to share all or part of the information in their account with other individuals that they designate, such as family members, and VA and non-VA health care providers.

In order to administer the My Health e Vet program and support the provision of the above benefits to Veterans, VHA retains administrative information, including personally identifiable information on users of My Health e Vet. In addition, VHA houses the patient's self-entered information in a separate database, but the administrative and patient data files can be linked. This administrative information is stored in the My Health e Vet Administrative Records System, and constitutes a separate system of records.

(FY 2011) PIA: VBA Minor Applications

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

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

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

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

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

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

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

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

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

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

ASISTS	Beneficiary Travel	Accounts Receivable	Adverse Reaction Tracking
Bed Control	Care Management	ADP Planning (PlanMan)	Authorization/ Subscription
CAPRI	Care Tracker	Bad Code Med Admin	Auto Replenishment/ Ward Stock
CMOP	Clinical Reminders	Clinical Case Registries	Automated Info Collection Sys
Dental	CPT/ HCPCS Codes	Clinical Procedures	Automated Lab Instruments
Dietetics	DRG Grouper	Consult/ Request Tracking	Automated Med Info Exchange
Fee Basis	DSS Extracts	Controlled Substances	Capacity Management - RUM
GRECC	Education Tracking	Credentials Tracking	Capacity Management Tools
HINQ	Engineering	Discharge Summary	Clinical Info Resource Network
IFCAP	Event Capture	Drug Accountability	Clinical Monitoring System
Imaging	Extensible Editor	EEO Complaint Tracking	Enrollment Application System
Kernal	Health Summary	Electronic Signature	Equipment/ Turn-in Request
Kids	Incident Reporting	Event Driven Reporting	Gen. Med.Rec. - Generator
Lab Service	Intake/ Output	External Peer Review	Health Data and Informatics
Letterman	Integrated Billing	Functional Independence	ICR - Immunology Case Registry
Library	Lexicon Utility	Gen. Med. Rec. - I/O	Income Verification Match
Mailman	List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine	Mental Health	Generic Code Sheet	Interim Mangement Support
MICOM	MyHealthEVet	Health Level Seven	X Master Patient Index VistA
NDBI	National Drug File	Hospital Based Home Care	Missing Patient Reg (Original) A4EL
NOIS	Nursing Service	Inpatient Medications	Order Entry/ Results Reporting
Oncology	Occurrence Screen	Integrated Patient Funds	PCE Patient Care Encounter
PAID	Patch Module	MCCR National Database	Pharmacy Benefits Mangement
Prosthetics	Patient Feedback	Minimal Patient Dataset	Pharmacy Data Management
QUASER	Police & Security	National Laboratory Test	Pharmacy National Database
RPC Broker	Problem List	Network Health Exchange	Pharmacy Prescription Practice
SAGG	Progress Notes	Outpatient Pharmacy	Quality Assurance Integration
Scheduling	Record Tracking	Patient Data Exchange	Quality Improvement Checklist
Social Work	Registration	Patient Representative	Radiology/ Nuclear Medicine
Surgery	Run Time Library	PCE Patient/ HIS Subset	Release of Information - DSSI
Toolkit	Survey Generator	Security Suite Utility Pack	Remote Order/ Entry System
Unwinder	Utilization Review	Shift Change Handoff Tool	Utility Management Rollup
VA Fileman	Visit Tracking	Spinal Cord Dysfunction	CA Verified Components - DSSI
VBECS	VistALink Security	Text Integration Utilities	Vendor - Document Storage Sys
VDEF	Women's Health	VHS & RA Tracking System	Visual Impairment Service Team ANRV
VistALink		Voluntary Timekeeping	Voluntary Timekeeping National

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

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

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

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

(FY 2011) PIA: Minor Applications

Which of these are sub-components of your system?		
1184 Web	ENDSOFT	RAFT
A4P	Enterprise Terminology Server & VHA Enterprise Terminology Services	RALS
Administrative Data Repository (ADR)	ePROMISE	Remedy Application
ADT	EYECAP	SAN
Agent Cashier	Financial and Accounting System (FAS)	Scanning Exam and Evaluation System
Air Fortress	Financial Management System	Sentillion
Auto Instrument	Genesys	Stellant
Automated Access Request	Health Summary Contingency	Stentor
BDN 301	ICB	Tracking Continuing Education
Bed Board Management System	KOWA	Traumatic Brain Injury
Cardiff Teleform	Lynx Duress Alarm	VA Conference Room Registration
Cardiology Systems (stand alone servers from the network)	MHTP	VAMedSafe
CHECKPOINT	Microsoft Active Directory	VBA Data Warehouse
Clinical Data Repository/Health Data Repository	Microsoft Exchange E-mail System	VHAHUNAPP1
Combat Veteran Outreach Committee on Waiver and Compromises	Military/Vet Eye Injury Registry	VHAHUNFPC1
CP&E	Mumps AudioFAX	VISTA RAD
Crystal Reports Enterprise	NOAHLINK	Whiteboard
Data Innovations	Omnicell	
DELIVEREX	Onvicord (VLOG)	
DICTATION-Power Scribe	Optifill	
DRM Plus	P2000 ROBOT	
DSIT	PACS database	
DSS Quadramed	Personal Computer Generated Letters	
EDS Whiteboard (AVJED)	PICIS OR	
EKG System	PIV Systems	
Embedded Fragment Registry	Q-Matic	
	QMSI Prescription Processing	

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	Meadows	
Description	How MHV gets data extracted from VistA and CPRS; middleware.	
Comments	Use ICN (internal control number) in VistA to identify user.	
Is PII collected by this minor application?		YES
Does this minor application store PII?		NO
If yes, where?		
Who has access to this data?	VA contractors.	

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

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

(FY 2011) PIA: Final Signatures

Facility Name: CDCO > AITC > VHA > My HealtheVet

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

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

Digital Signature Block

Information Security Officer:	Paula Pinckney	(301) 734-0438	Paula.Pinckney@va.gov
-------------------------------	----------------	----------------	-----------------------

Digital Signature Block

System Owner/ Chief Information Officer:	John Rucker	(512) 326-6000	John.Rucker@va.gov
--	-------------	----------------	--------------------

Digital Signature Block

OI&T OED Project Manager	Patricia Simon	(315) 587-6014	Patricia.Simon2@va.gov
--------------------------	----------------	----------------	------------------------

Digital Signature Block

Information Owner (VHA)	Theresa Hancock	(301) 734-0371	Theresa.Hancock@va.gov
-------------------------	-----------------	----------------	------------------------

Digital Signature Block

Business Owner	Madhulika Agarwal	(202) 461-7590	Madhulika.Agarwal.va.gov
----------------	-------------------	----------------	--------------------------

Digital Signature Block

Other Titles: AITC Project Manager

James Magness

(512) 326-6282

James.Magness@va.gov

Digital Signature Block

Date of Report:

11/1/10

OMB Unique Project Identifier

029-00-01-11-01-1242-00

Project Name

CDCO > AITC > VHA > My
HealthVet

(FY 2011) PIA: Final Signatures

Facility Name: AITC

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

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

Digital Signature Block

Information Security Officer:

Digital Signature Block

System Owner/Chief Information Officer:	John Rucker	512-326-6422	John.Rucker@va.gov
---	-------------	--------------	--


Digital Signature Block

Information Owner:

Digital Signature Block

Other Titles:

Digital Signature Block

Date of Report:

OMB Unique Project Identifier

Project Name