

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

Submitting PIA's into SMART

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:	Region 3>VHA>VISN07>Birmingham VAMC>VistA		
OMB Unique System / Application / Program Identifier (AKA: UPID #):	029-00-01-11-01-1180-00		
Description of System/ Application/ Program:	<p>The VistA-Legacy system is the software platform and hardware infrastructure (associated with clinical operations) on which VHA health care facilities operate their software applications and support for E-Government initiatives. It includes the computer equipment associated with clinical operations and the employee (approximately 2500 FTE) necessary to operate the system. VistA-Legacy is a client-server system. It links the facility computer network to over 100 applications and databases. VistA-Legacy provides critical data that supports the delivery of healthcare to veterans and their dependants. Using the computer, the VA health care provider can access VistA-Legacy applications and meet a wide range of healthcare data needs. The VistA-Legacy system operates in medical centers, ambulatory and community-based clinics, nursing homes and domiciliaries. The VistA-Legacy system is in the mature phase of the capital investment lifecycle.</p>		
Facility Name:	521 Birmingham VAMC		
Title:	Name:	Phone:	Email:
Privacy Officer:	Kim Moses	205-212-3162	kim.moses@va.gov
Information Security Officer:	James Reynolds	205-558-7039	james.reynolds4@va.gov
System Owner/ Chief Information Officer:	William Greer	205-933-8101	william.greer2@va.gov
Information Owner:			
Other Titles:			
Person Completing Document:	Kim Moses	205-212-3162	kim.moses@va.gov
Person Completing Document:	James Reynolds	205-558-7039	james.reynolds4@va.gov
Person Completing Document:	William Greer	205-933-8101	william.greer2@va.gov
Other Titles:			
Date of Last PIA Approved by VACO Privacy Services: (01/2008)			
Date Approval To Operate Expires:	08/2011		
What specific legal authorities authorize this program or system:	Title 38, United StatesCode, Section 7301(a)		
What is the expected number of individuals that will have their PII stored in this system:	1,000,000 - 9,999,999		
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.	27 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):	03/2011		
Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.			
<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/DHI data?			
<input checked="" type="checkbox"/> 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):	79VA19
2. Name of the System of Records:	Veterans Health Information Systems and Technology Architecture (Vista) Records - VA
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm
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
	<i>(Please Select Yes/No)</i>
Is PII collected by paper methods?	Yes
Is PII collected by verbal methods?	Yes
Is PII collected by automated methods?	Yes
Is a Privacy notice provided?	Yes
Proximity and Timing: Is the privacy notice provided at the time of data collection?	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)	ALL	Data will be used to identify the veteran determine eligibility for care, schedule treatment, MCCR activities, and manage the provided care.	Verbal & Written	Verbal & Written
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Benefits, Healthcare	Verbal & Written	Verbal & Written
Service Information	ALL	Military Service Information (Branch of service, discharge date, discharge type, service connection rating, medical conditions related to military service, etc). This information is collected to assess eligibility for VA healthcare benefits, type of healthcare needed.	Verbal & Written	Verbal & Written
Medical Information	ALL	VistA-Legacy applications meet a wide range of health care data needs. The VistA-legacy system operates in medical centers, ambulatory and community-based clinics, nursing homes and domiciliary, and thus collects a wide range of personal medical information for clinical diagnosis, treatment, patient evaluation, and patient care. common types of personal medical information would include lab test results, prescriptions, allergies, medical diagnoses, vital signs, etc. The information is used to treat and care for the veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of the veteran.	Verbal & Written	Verbal & Written
Criminal Record Information	ALL	Fugitive/Felon Information is used to determine veteran's eligibility to continue receiving medical care and billing purposes.	Verbal & Written	Verbal & Written

(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	VBA, Cemetary, HEC	Yes	Used to communicate/verify patient eligibility. Montgomery VA Regional Office has access to patient information to assist with adjudication with VA Beneficiary Claims. Veterans Cemetery Administration to determine patient's eligibility for burial at specific locations. Health Revenue Center has access to handle first party billing concerns.	Both PII & PHI	VHA Handbook 1601.1 and 1605.1
Other Veteran Organization	VSO	No	Eligibility	Both PII & PHI	Privacy Act, VA Form 10-5345, VHA Handbook 1601.1, 15. Processing a Request
Other Federal Government Agency	IRS, SSA, DoD, CMS	No	Income verifications for MCCR and eligibility for care. Verification of insurance and payment status	Both PII & PHI	Privacy Act, VA Form 1053-45, VHA Handbook 1605.1
State Government Agency	Public Health, Dept of Human Resources Vital Statistics, law enforcement	No	Used to determine communicabl ediseases and dates of birth/death for assistance with nursing, home placement and abuse cases and public safety	Both PII & PHI	Standing letter, VHA Handbook 1605.1
Local Government Agency	Health, law enforcement	No	Public health and safety		Standing letter, VHA Handbook 1605.1
Research Entity	As requested	No	Research activities	PHI	Valid HIPAA Authorization or HIPAA Waiver
Other Project / System	Blue Cross/Blue Shield of Alabama	No	Verification of insurance and payment status	Both PII & PHI	Birmingham MCM 136-14, VHA Handbook 1605.1; HIPAA
Other Project / System	State Veterans Nursing Home	No	Treatment purposes and continuation of care	PHI	Privacy Act, HIPAA, VHA Handbook 1605.1
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system? No

Please enter the name of the system: _____

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

Is there a contingency plan in place to pr

(FY 2011) PIA: Secondary Us

Will PII data be included with any secon

if yes, please check all that apply: Online vi Sickle Cell orm HIV

Describe process for authorizing access t

Answer: HIPAA authorization/Waiver of

(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: Indexing	
How is data checked for completeness?	
Answer: Quality Control	
What steps or procedures are taken to ensure the data remains current and not out of date?	
Answer: Ongoing updating with each Veteran contract.	
How is new data verified for relevance, authenticity and accuracy?	
Answer: Verify with Veterans/patients, signed and authenticated by Provider, signature blocks	
<i>Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)</i>	
Answer:	
(FY 2011) PIA: Retention & Disposal	
What is the data retention period?	
Answer: Electronic Final Version of Patient Medical Record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records control Schedule 10-1, Item XLIII, 2.b. At the present itme, VistA Imaging retains all images.	
Explain why the information is needed for the indicated retention period?	
Answer: Health care operations, treatment and payment	
What are the procedures for eliminating data at the end of the retention period?	
Answer: VA Handbook 6300.1, pgs 24-25 7. Destruction of Records. Records are destroyed utilizing shredding contractor. Contractor picks up documents on a defined schedule for the facility and CBOCs.	
Where are these procedures documented?	
Answer: Local MCM - Paperwork Management, VA Handbook 6300, Record Control Schedule 10-1	
How are data retention procedures enforced?	
Answer: VA Records control Schedule 10-1 (page 8): Records Management Responsibilities; the Health Information Resources Service (HIRS) is responsible for developing policies and procedures for effective and efficient records management throughout VHA. In addition, HIRS acts as the liaison between VHA and the National Archives and Records Administration (NARA) on issues pertaining to records management practices and procedures. Field records officers are responsible for records management activities at their facility. Program officials are responsible for creating, maintaining, protecting, and disposing of records in their program area in accordance with NARA regulations and VA policy. All VHA employees are responsible to ensure that records are created, maintained, protected and disposed of in accordance with NARA regulations and VA policies and procedures.	
Has the retention schedule been approved by the National Archives and Records Administration (NARA)	Yes
<i>Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)</i>	
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: The VistA System is in the operational phase and completes a full C&A every three years. Continuous Monitoring is occurring on the system on an annual basis. There is currently an ATO valid through August 2011.

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

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

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

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: Controls to mitigate misuse, security controls, Security Controls Assessment, Continuous Monitoring

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. Please indicate the question you are responding to and then add your comments.

(FY 2011) 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)
Appraisal System	Benefits Delivery Network (BDN)	Automated Medical Information System (AMIS)290
ASSISTS	Centralized Property Tracking System	Automated Standardized Performance Elements Nationwide (ASPEN)
Awards	Common Security User Manager (CSUM)	Centralized Accounts Receivable System (CARS)
Awards	Compensation and Pension (C&P)	Committee on Waivers and Compromises (COWC)
Baker System	Control of Veterans Records (COVERS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
bbraun (CP Hemo)	Control of Veterans Records (COVERS)	Compensation & Pension Training Website
BDN Payment History	Control of Veterans Records (COVERS)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
BIRLS	Courseware Delivery System (CDS)	Distribution of Operational Resources (DOOR)
C&P Payment System	Dental Records Manager	Educational Assistance for Members of the Selected Reserve Program CH 1606
C&P Training Website	Education Training Website	Electronic Performance Support System (EPSS)
CONDO PUD Builder	Electronic Appraisal System	Enterprise Wireless Messaging System (Blackberry)
Corporate Database	Electronic Card System (ECS)	Financial Management Information System (FMI)
Data Warehouse	Electronic Payroll Deduction (EPD)	Hearing Officer Letters and Reports System (HOLAR)
EndoSoft	Eligibility Verification Report (EVR)	Inquiry Routing Information System (IRIS)
FOCAS	Fiduciary Beneficiary System (FBS)	Modern Awards Process Development (MAP-D)
Inforce	Fiduciary STAR Case Review	Personnel and Accounting Integrated Data and Fee Basis (PAID)
INS - BIRLS	Financial and Accounting System (FAS)	Personal Computer Generated Letters (PCGL)
Insurance Online	Insurance Unclaimed Liabilities	Personnel Information Exchange System (PIES)
Insurance Self Service	Inventory Management System (IMS)	Personnel Information Exchange System (PIES)
LGY Home Loans	LGY Centralized Fax System	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing	Loan Service and Claims	Purchase Order Management System (POMS)
Mobilization	Loan Guaranty Training Website	Reinstatement Entitlement Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Assistant	Service Member Records Tracking System
Omnicell	National Silent Monitoring (NSM)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Powerscribe Dictation System	Systematic Technical Accuracy Review (STAR)
RAI/MDS	Rating Board Automation 2000 (RBA2000)	Training and Performance Support System (TPSS)
Right Now Web	Rating Board Automation 2000 (RBA2000)	VA Online Certification of Enrollment (VA-ONCE)
SAHSHA	Rating Board Automation 2000 (RBA2000)	VA Reserve Educational Assistance Program
Script Pro	Records Locator System	Veterans Appeals Control and Locator System (VACOLS)
SHARE	Review of Quality (ROQ)	Veterans Assistance Discharge System (VADS)
SHARE	Search Participant Profile (SPP)	Veterans Exam Request Info System (VERIS)
SHARE	Spinal Bifida Program Ch 18	Veterans Service Representative (VSR) Advisor
Sideaxis	State Benefits Reference System	Vocational Rehabilitation & Employment (VR&E) CH 31
Synquest	State of Case/Supplemental (SOC/SSOC)	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
VBA Data Warehouse	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	Veterans On-Line Applications (VONAPP)	Web Automated Verification of Enrollment
VIC	Veterans Service Network (VETSNET)	Web-Enabled Approval Management System (WEAMS)
VR&E Training Website	Web Electronic Lender Identification	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 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

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

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

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

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

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

(FY 2011) PIA: Minor Applications

Which of these are sub-components of your system?		
1184 Web	ENDSOFT	RAFT
A4P	Enterprise Terminology Server & VHA Enterprise Terminology Services	RALS
x Administrative Data Repository (ADR)	ePROMISE	Remedy Application
x ADT	EYECAP	SAN
x Agent Cashier	Financial and Accounting System (FAS)	Scanning Exam and Evaluation System
x Air Fortress	Financial Management System	Sentillion
Auto Instrument	Genesys	Stellant
x Automated Access Request	Health Summary Contingency	Stentor
BDN 301	ICB	Tracking Continuing Education
x 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
x CHECKPOINT	Microsoft Active Directory	VBA Data Warehouse
x Clinical Data Repository/Health Data Repository	Microsoft Exchange E-mail System	VHAHUNAPP1
x Combat Veteran Outreach Committee on Waiver and Compromises	Military/Vet Eye Injury Registry	VHAHUNFPC1
CP&E	Mumps AudioFAX	VISTA RAD
x Crystal Reports Enterprise	NOAHLINK	Whiteboard
Data Innovations	Omicell	
DELIVEREX	Onvicord (VLOG)	
x DICTATION-Power Scribe	Optifill	
x DRM Plus	P2000 ROBOT	
x DSIT	PACS database	
x 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
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: Final Signatures

Facility Name: Region 3>VHA>VISN07>Birmingham VAMC>VistA

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

Privacy Officer:	Kim Moses	205-212-3162	kim.moses@va.gov
------------------	-----------	--------------	------------------

Digital Signature Block

Information Security Officer:	James Reynolds	205-558-7039	james.reynolds4@va.gov
-------------------------------	----------------	--------------	------------------------

Digital Signature Block

System Owner/ Chief Information Officer:	William Greer	205-933-8101, x 7070	william.greer2@va.gov
--	---------------	-------------------------	-----------------------

Digital Signature Block

Information Owner:	0	0	0
--------------------	---	---	---

Digital Signature Block

Other Titles:	0	0	0
---------------	---	---	---

Digital Signature Block

Date of Report: 3/31/11
 OMB Unique Project Identifier 029-00-01-11-01-1180-00
 Region
 3>VHA>VISN07>Birmingham
 Project Name VAMC>VistA