

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: Region 3 > VHA > VISN 6 > Beckley VAMC > VISTA
 OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-01-11-01-1180-00
 Description of System/ Application/ Program: This system is designed to operate as a fully integrated clinical and administrative information system that processes clinical information, information covered by the Privacy Act & HIPAA, PHI/ePHI, financial records, and all other data necessary to run a tertiary medical center. All clinical and most administrative functions within the physical confines of the VISN8 utilize the VistA Alpha cluster to process clinical, financial, or administrative data. All external organizations which access a local Alpha node must be authenticated by access and verify codes or by domain transmission scripts for electronic mail. Examples of these organizations include VBA Regional Office, Form, HINQ, all VA facilities throughout the country sending electronic mail,

Facility Name: Beckley VAMC

Title:	Name:	Phone:	Email:
Privacy Officer:	Elizabeth Becker	304-255-2121 x4465	elizabeth.becker@va.gov
Information Security Officer:	William Shepperd	304-255-2121 x4962	william.shepperd@va.gov
System Owner/ Delegation of Authority	Sherry Gregg	304-255-2121 x4046	sherry.gregg@va.gov
Other Titles: VISTA System Manager	Greg Angell	304-255-2121 x4124	gregory.angell@va.gov
Other Titles:	N/A	N/A	N/A
Person Completing Document:	William Shepperd	304-255-2121 x4962	william.shepperd@va.gov
Other Titles:	N/A	N/A	N/A
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 USC
 What is the expected number of individuals that will have their PII stored in this system: 1-9,999,999
 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. Approximately 25 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): 7/8/2011

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

- Have any changes been made to the system since the last PIA?
- Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- Does this system/application/program collect, store or disseminate PII/PHI data?
- Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please complete TAB 2 & 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

79VA19 - Veterans Health Information Systems and Technology Architecture (Vista) Records-VA and the legal authority is: Title 38, United States Code, section 7301(a).

2. Name of the System of Records:

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

<http://vawww.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

(Please Select Yes/No)

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	This data will be used by management and for provision of healthcare, healthcare operations, billing of patient care episodes, mailing lists for research, provision of new services, recalls of medications, quality assurance of health care activities, and public health surveillance. When data is collected for research project, the uses of data vary. Patients will be informed of all general uses of data. Where a specific risk will be encountered, the patient will be requested to sign an informed consent which notifies them in writing (in addition to the verbal summation) of known risks. The subject will be informed of all risks, uses, users, and whether or not he/she will benefit from the project.	All	All
Family Relation (spouse, children, parents, grandparents, etc)	Paper & Electronic	The data will be used primarily for research purposes. The subjects will be notified of all risks, uses, and users of the data. When used for health care operations, demographics of family are used for contacting in an alternate decision maker in the event the patient is incapacitated and rarely for infectious disease surveillance.	All	All

Service Information	ALL	The individual will be notified that the data may be used to verify eligibility for care (or specific services) in the VA system. Occasionally a service record is important as part of the patient's medical history required for diagnosis. When this occurs, the patient will be told their service record is being reviewed. When used for research, the purpose of the research. Sometimes the Institutional review Board will approve waiver of informed consent. This is typically used with retrospective studies.	All	All
Medical Information	ALL	The patient is told in the VA's Notice of Privacy Practices that their information will be used for diagnosis and treatment, eligibility and enrollment, quality improvement, public health surveillance, abuse reporting, patient directories, as required by law, workers compensation cases, services, health care operations, training of medical students, oversight and accreditation and billing.	All	All
Criminal Record Information	Electronic/File Transfer	Patients are notified that information will be used as required by law and for criminal investigations and matters of National Security	Written	Written
Guardian Information	ALL	Patients are informed that this data is needed for research, funeral matters, billing, health care operations, abuse reporting, and social work support. When the data will be used for research in most cases, an informed consent will be obtained from the guardian, or the data will be collected under an Institutional Review Board waiver.	All	All

Education Information	ALL	I collected for research, the individual will be told the specific reasons why this data will be requested. If the individual is a workforce member, the training is mandatory and they are notified of this in the process of taking the training.	Verbal & Automatic	Automated
Benefit Information	ALL	the patient is informed that the data is required for eligibility and enrollment.	All	All
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory	Verbal or written informed consent
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	Verbal or written informed consent
Service Information	Yes	Veteran	Mandatory	Verbal or written informed consent
Medical Information	Yes	Veteran	Mandatory	Verbally, on the phone, automated, and paper.
Criminal Record Information	Yes	Other (Explain)	Voluntary	Verbal or written informed consent
Guardian Information	Yes	Veteran	Voluntary	Verbal or written informed consent
Education Information	Yes	Veteran	Voluntary	Verbal or written informed consent
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	Verbal or written informed consent

Education Information for workforce
members

Yes

Other (Explain)

Mandatory

Verbally as part of
orientation

Other (Explain)

Other (Explain)

(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	No	No	N/A	N/A	
Other Veteran Organization	No	No	N/A	N/A	
Other Federal Government Agency	Yes	No	VHA VISTA patient data is shared with DOD and CDC in compliance with federal law.	Both PII & PHI	
State Government Agency	No	No	N/A	N/A	
Local Government Agency	No	No	N/A	N/A	
Research Entity	No	No	N/A	N/A	
Other Project / System					
Other Project / System					
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
 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? No

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

if yes, please check all that apply:

Describe process for authorizing access to this data.

Answer: N/A

(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: Patient health information if disclosed could

Explain how collected data are limited to required elements:

Answer: Access to the VISTA system is on a need to access/need to know basis. Only authorized personnel are granted access to the system and their access is restricted in accordance with least privilege.

How is data checked for completeness?

Answer: Patients check in via the central intake office. At this time patients must verify their information. Also, patients information is verified via release of information and in clinical visits to ensure accuracy.

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

Answer: Administrative data is updated with each application for care. Each time a veteran is seen for an appointment, hospitalization, travel pay, etc. Data is verified and updated at the time the patient presents for care or follow-up. For example, clinics verify address, next of kin and insurance information.

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

Answer: New data is compared with printed form or via patient verification. The veteran brings DD214 with them and it is verified. For example, the 1010 is printed and the veteran reviews and signs that the information is accurate. For example, the VISTA system is designed to identify inconsistencies in data that is reported and provides an exception list for several applications

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

Answer: N/A

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: The retention period is dependent on the type of data and the intended use, so retention period varies. 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 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 facilities. Program officials are responsible for creating, maintaining, protecting, and disposing of records in their program area in accordance with MARA 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. Local policy Medical Center Memorandum 590-136-19 "Records Management Policy".

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

Answer: Mandatory requirements are set for each type of data stored.

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

Answer: Applicable federal regulatory requirements will be followed for eliminating or disposing of data.

Where are these procedures documented?

Answer: VA Handbook 6300; Record Control Schedule 10-1

How are data retention procedures enforced?

Answer: Procedures will be enforced using technical and managerial control mechanisms. Local Records Management Policy, Medical Center Memorandum 590-136-19 "Records Management Policy".

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

No

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: The system's security controls are certified every three years by an independent entity. The system owner, the Regional Information Officer reviews the recommendations and authorizes the system if appropriate. Plans of Action and Milestones are created and reviewed quarterly until closure. An annual risk assessment is conducted to detect changes in security controls and any newly identified vulnerabilities are added to the national database, Security Management And Reporting Tool. Plans of Actions and Milestones are created for these vulnerabilities. Also Information Technology Oversight and Compliance as well as the Office of the Inspector General review the system after the triennial Certification and Accreditation process is complete to validate the Plans of Actions and Milestones and the security controls that were certified as compliant.

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 checked="" type="checkbox"/> Chemical/Biological Contamination | <input checked="" type="checkbox"/> Data Integrity Loss | <input checked="" type="checkbox"/> Identity Theft |
| <input checked="" type="checkbox"/> Blackmail | <input checked="" type="checkbox"/> Denial of Service Attacks | <input checked="" 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 checked="" type="checkbox"/> Substance Abuse |
| <input checked="" type="checkbox"/> Computer Intrusion | <input checked="" type="checkbox"/> Flooding/Water Damage | <input checked="" type="checkbox"/> Theft of Assets |
| <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 checked="" 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, no choices were made regarding the project/system or collection of information as a result of performing the PIA.

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	X Automated Medical Information Exchange II (AIME II)
Appraisal System	Benefits Delivery Network (BDN)	Automated Medical Information System (AMIS)290
X ASSISTS	Centralized Property Tracking System	Automated Standardized Performace 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)	X 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 Entitelment Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Asisstant	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
Sidexis	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	ADP Planning (PlanMan)	X Authorization/ Subscription
X CAPRI	Care Tracker	X Bad Code Med Admin	X Auto Replenishment/ Ward Stock
X CMOP	X Clinical Reminders	X Clinical Case Registries	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	X Capacity Management - RUM
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	Clinical Monitoring System
X Imaging	X Extensible Editor	X EEO Complaint Tracking	X Enrollment Application System
X Kernal	X Health Summary	X Electronic Signature	X Equipment/ Turn-in Request
X Kids	X Incident Reporting	X Event Driven Reporting	Gen. Med.Rec. - Generator
X Lab Service	Intake/ Output	X External Peer Review	X Health Data and Informatics
Letterman	X Integrated Billing	X Functional Independence	X ICR - Immunology Case Registry
X 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	Patch Module	X MCCR National Database	X Pharmacy Benefits Mangement
X Prosthetics	Patient Feedback	X Minimal Patient Dataset	X Pharmacy Data Management
X QUASER	X Police & Security	National Laboratory Test	Pharmacy National Database
X RPC Broker	X Problem List	X Network Health Exchange	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	Utilization Review	X Shift Change Handoff Tool	X Utility Management Rollup
X VA Fileman	X Visit Tracking	X Spinal Cord Dysfunction	CA Verified Components - DSSI
X VBECS	X VistALink Security	X Text Integration Utilities	X Vendor - Document Storage Sys
VDEF	X Women's Health	VHS & RA Tracking System	X Visual Impairment Service Team ANRV
X VistALink		X 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 VAMedSafe
Cardiology Systems (stand alone servers from the network)	MHTP	
CHECKPOINT	Microsoft Active Directory	VBA Data Warehouse
Clinical Data Repository/Health Data Repository	Microsoft Exchange E-mail System	VHAHUNAPP1 VHAHUNFPC1
Combat Veteran Outreach Committee on Waiver and Compromises	Military/Vet Eye Injury Registry	VISTA RAD
CP&E	Mumps AudioFAX	Whiteboard
Crystal Reports Enterprise	NOAHLINK	
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
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 > VISN 6 > Beckley VAMC > VISTA

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

Privacy Officer:

Digital Signature Block

Information Security Officer:

Digital Signature Block

System Owner/ Delegation of Authority

Digital Signature Block

Other Titles: VISTA System Manager

Digital Signature Block

Other Titles: N/A N/A N/A

Digital Signature Block

Date of Report: 7/11/11

OMB Unique Project Identifier 029-00-01-11-01-1180-00

Project Name Region 3 > VHA > VISN 6 > Beckley

VAMC > VISTA

(FY 2011) PIA: Final Signatures

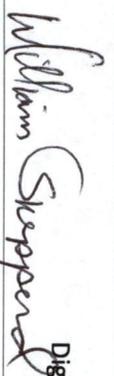
Facility Name: REGION3>VHA>VISN6>BECKLEYVAMC>VISTA

Title: Name: Phone: Email:

Privacy Officer: Elizabeth Becker 304-255-2121, Ext. 4465 elizabeth.becker@va.gov


Digital Signature Block

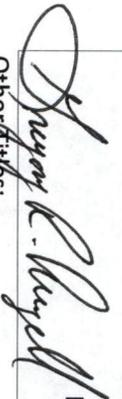
Information Security Officer: William Shepperd 304-255-2121, Ext. 4962 william.shepperd@va.gov


Digital Signature Block

System Owner/ Chief Information Officer: Sherry Gregg 304-255-2121, Ext. 4046 sherry.gregg@va.gov


Digital Signature Block

Information Owner: Gregory Angell 304-255-2121, Ext. 4665 gregory.angell@va.gov


Digital Signature Block

Other Titles: 0 0


Digital Signature Block

Date of Report: 3/23/11

OMB Unique Project Identifier 029-00-01-11-01-1180-00

Project Name REGION3>VHA>VISN6>BECKLEYVA

MC>VISTA