

Welcome to the PIA for FY 2010!

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. More information can be found by reading VA 6508.

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 Privacy Impact Assessment Handbook 6202.2 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 Handbook 6202.2.
- 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 Handbook 6202.2 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

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, indirectly 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

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.

(FY 2010) PIA: System Identification

Program or System Name: REGION3>VHA>VISN 7> Charlie Norwood VAMC> VistA Legacy

OMB Unique System / Application / Program

Identifier (AKA: UPID #): 029-00-01-11-01-1180-00

Description of System / Application / Program: The VistA-Legacy system is the software platform and hardware infrastructure (associated with clinical operations) on which the 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 employees (approximately 2300 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. In 2006, the VistA-Legacy system supported IT services across the VA organization which had a network of 21 Veterans Integrated Service Networks (VISNs) that managed 155 medical centers, over 881 community based outpatient clinics, 46 residential rehabilitation treatment programs, 135 nursing homes, 207 readjustment counseling centers, 57 veteran benefits regional offices and 125 national cemeteries. 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 health care data needs. The VistA-Legacy system operates in medical centers, ambulatory and community-based clinics, nursing homes and domiciliary. The VistA-Legacy system is in the mature phase of the capital investment life cycle.

Facility Name: Charlie Norwood VA Medial Center (509)

Title:	Name:	Phone:
Privacy Officer:	Shawana Burch	(706) 733-0188
Information Security Officer:	Sue Heath	(706) 481-6743
Chief Information Officer:	Gerald Crawford	(706) 481-6750
Person Completing Document:	Shawana Burch	(706) 733-0188
Other Titles: VistA System Manager	Rebecca Swords	(706) 481-6775

Other Titles:

Other Titles:

Date of Last PIA Approved by VACO Privacy

Services: (MM/YYYY) 08/2008

Date Approval To Operate Expires: 08/2011

What specific legal authorities authorize this program or system: Title 38, United States Code, 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. Operational 26 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): 08/2008

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 skip to TAB 12. (See Comment for Definition of PII)

Email:

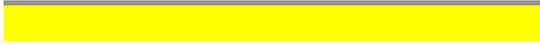
shawana.burch@va.gov

sue.Heath@va.gov

Gerald.Crawford@va.gov

shawana.burch@va.gov

Rebecca.Swords@va.gov



ng work fc



(FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?

Yes

if the answer above is no, please skip to row 16.

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

- | | |
|---|---|
| 1. All System of Record Identifier(s) (number): | 79VA19 |
| 2. Name of the System of Records: | VistA-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

(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 2010) 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	Eligibility, Benefits, Healthcare	All	All
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Eligibility, Benefits	All	All
Service Information	ALL	Eligibility, Benefits	All	All
Medical Information	ALL	Healthcare, Research, Benefits	All	All
Criminal Record Information	Paper & Electronic	Eligibility, Billing	All	All
Guardian Information	Paper & Electronic	Healthcare	Verbal & Written	Verbal & Written
Education Information	Paper & Electronic	Healthcare, Billing	Verbal & Written	Verbal & Written
Benefit Information	Paper & Electronic	Eligibility, Benefits, Employment	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	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Mandatory	
Service Information	Yes	Veteran	Mandatory	
Medical Information	Yes	Veteran	Mandatory	
Criminal Record Information	Yes	VA Files / Databases (Identify file)	Mandatory	Fugitive Felon Program
Guardian Information	Yes	Veteran	Mandatory	
Education Information	Yes	Veteran	Mandatory	
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	VBA
Other (Explain)				
Other (Explain)				

Other (Explain)

(FY 2010) 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	VA Regional Office (VARO)(Atlanta and Columbia)	Yes	VARO: SSN, Date of Birth and sex for the adjudication of VA beneficiary claims	Both PII & PHI	VHA Handbooks 1605.1 and VHA 1605.2
Other Veteran Organization		No			
Other Federal Government Agency	Social Security Administration; Internal Revenue Service (IRS); Centers for Disease Control (CDC);	No	VARO and SSA: Name, SSN, Date of Birth and sex for the adjudication of VA beneficiary claims, SSA disability determination, and income verification; IRS: PII for verification of income for billing purposes; CDC: PII and PHI for healthcare reporting	Both PII & PHI	VHA Handbooks 1605.1 and VHA 1605.2
State Government Agency		No		N/A	
Local Government Agency		No		N/A	
Research Entity		No		N/A	
Other Project / System	Federal Bidirectional Health Information Exchange (FHIE/BHIE)	Yes	PII and PHI for the provision of healthcare to veterans and active duty soldiers	Both PII & PHI	VHA Handbooks 1605.1 and VHA 1605.2
Other Project / System	Eisenhower Army Medical Center (EAMC)	Yes	PII and PHI for the provision of healthcare to veterans and active duty soldiers	Both PII & PHI	VHA Handbooks 1605.1 and VHA 1605.2
Other Project / System					

(FY 2010) 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 2010) PIA: Secondary Use

Will PII data be included with any secondary use request? No

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:

(FY 2010) 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: Data is collected electronically based on the automation of VA forms and clinical procedures.

How is data checked for completeness?

Answer: Data is reviewed by staff and compared to paper forms and verified with veteran.

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

Answer: Clinical data is not removed. Administrative data is updated with each application for care.

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

Answer: New data is compared with printed form or via patient verification.

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

Answer:

(FY 2010) PIA: Retention & Disposal

What is the data retention period?

Answer: Clinical information is retained at the treating facility for three years. If no activity is recorded in three years the record is converted to inactive. If inactive for one year, the record is transferred to the Federal Record Center for storage. If not recalled, the records are destroyed 72 years after retirement or 75 years after last episode of care. Record is maintained for a document of record.

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

Answer: Data is maintained in accordance with VA Directive 6300,

http://vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&FTYPE=2, VA Handbook 6300.1,

http://vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&FTYPE=2, and VHA Records

Control Schedule(RCS) 10-1, http://vaww1.va.gov/VHA_publications/rcs10/rcs10-1.pdf. The final,

consolidated, electronic version of a Patient Medical Record, including information migrated from interim electronic information systems, electronic medical equipment, or information entered directly into the patient medical record information system is destroyed/deleted 75 years after the last episode of patient care, in accordance with RCS 10-1, XLIII, 2.b., Electronic Final Version of Health Record. Veterans Health Administration (VHA) RCS 10-1 is the main authority for the retention disposition of VHA records. It provides a brief description of the records and states the retention and disposition requirements. It also provides the National Archives and Records Administration (NARA) disposition authorities or the General Records Schedules (GRS) authorities, whichever is appropriate for the records. In addition to program and services sections, the RCS 10-1 contains a General and Administrative (G&A) Section for records common to several offices and services. Retention periods for data stored vary according to the type of records. Data owners are responsible for ensuring they follow the records retention periods outlined in RCS 10-1.

Answer: Data is maintained in accordance with VA Directive 6300,

http://vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&FTYPE=2, VA Handbook 6300.1,

http://vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&FTYPE=2, and VHA Records

What are the procedures for eliminating data at the end of the 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. (Page 190). At the present time, VistA Imaging retains all images.

Where are these procedures documented?

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

How are data retention procedures enforced?

Answer: VA Records Control Schedule 10-1 (page8): 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 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 for the disposition of Records.

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 2010) 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 2010) 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? No

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: Security testing performed annually as required by Handbook 6500

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: At the Department level the CIO's of Cyber & Information Security (OCIS) is responsible for the establishment of directives, policies, and procedures which are consistent with the provisions of Federal Information Security Management Act (FISMA) as well as guidance issued by the Office of Management & Budget (OMB), the National Institute of Standards & Technology (NIST), and other requirements that VistA-Legacy is and has been subject to. In addition, OCIS administers and manages Department-wide security solutions, such as anti-virus protection, authentication, vulnerability scanning and penetration testing, and intrusion detections, and incident response (800-61). At the VistA-Legacy project level – The Project Manager ensures that CIO-provided security directives are integrated into the project's security plan and implemented by VA and contractor staff throughout the project. Funding needs are dependent on IT security requirements identified in the system development life cycle (800-64) (i.e. risk assessments (800-30), certification and accreditation (800-37 and 800-53), as well as identified security weaknesses that must be corrected.

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

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

Answer: (Other Risks)

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

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

Answer: (Other Controls) : System and communication protection (SC); and system and information integrity (SI)

PIA: PIA Assessment

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

Answer: Review and reconciliation of local policy settings versus settings related in SSP

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 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.

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 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.

The controls are being considered for the project based on the selections from the previous assessments?

Please add additional controls:

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

(FY 2010) PIA: Additional Comments

Add any additional comments on this tab for any question in the form you want to comment on.
Please indicate the question you are responding to and then add your comments.

(FY 2010) PIA: VBA Minor Applications

Explain what minor application that are associated with your installation? (Check all that apply)

Records Locator System	Education Training Website	Appraisal System
Veterans Assistance Discharge System (VADS)	VR&E Training Website	Web Electronic Lender Identification
LGY Processing	VA Reserve Educational Assistance Program	CONDO PUD Builder
Loan Service and Claims	Web Automated Verification of Enrollment	Centralized Property Tracking System
LGY Home Loans	Right Now Web	Electronic Appraisal System
Search Participant Profile (SPP)	VA Online Certification of Enrollment (VA-ONCE)	Web LGY
Control of Veterans Records (COVERS)	Automated Folder Processing System (AFPS)	Access Manager
SHARE	Personal Computer Generated Letters (PCGL)	SAHSHA
Modern Awards Process Development (MAP-D)	Personnel Information Exchange System (PIES)	VBA Data Warehouse
Rating Board Automation 2000 (RBA2000)	Rating Board Automation 2000 (RBA2000)	Distribution of Operational Resources (DOOR)
State of Case/Supplemental (SOC/SSOC)	SHARE	Enterprise Wireless Messaging System (Blackberry)
Awards	State Benefits Reference System	VBA Enterprise Messaging System
Financial and Accounting System (FAS)	Training and Performance Support System (TPSS)	LGY Centralized Fax System
Eligibility Verification Report (EVR)	Veterans Appeals Control and Locator System (VACOLS)	Review of Quality (ROQ)
Automated Medical Information System (AMIS)290	Veterans On-Line Applications (VONAPP)	Automated Sales Reporting (ASR)
Web Automated Reference Material System (WARMS)	Automated Medical Information Exchange II (AIME II)	Electronic Card System (ECS)
Automated Standardized Performance Elements Nationwide (ASPEN)	Committee on Waivers and Compromises (COWC)	Electronic Payroll Deduction (EPD)
Inquiry Routing Information System (IRIS)	Common Security User Manager (CSUM)	Financial Management Information System (FMI)
National Silent Monitoring (NSM)	Compensation and Pension (C&P) Record Interchange (CAPRI)	Purchase Order Management System (POMS)
Web Service Medical Records (WebSMR)	Control of Veterans Records (COVERS)	Veterans Canteen Web
Systematic Technical Accuracy Review (STAR)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)	Inventory Management System (IMS)
Fiduciary STAR Case Review	Fiduciary Beneficiary System (FBS)	Synquest
Veterans Exam Request Info System (VERIS)	Hearing Officer Letters and Reports System (HOLAR)	RAI/MDS
Web Automated Folder Processing System (WAFPS)	Inforce	ASSISTS
Courseware Delivery System (CDS)	Awards	MUSE
Electronic Performance Support System (EPSS)	Actuarial	Bbraun (CP Hemo)
Veterans Service Representative (VSR) Advisor	Insurance Self Service	VIC
Loan Guaranty Training Website	Insurance Unclaimed Liabilities	BCMA Contingency Machines
C&P Training Website	Insurance Online	Script Pro

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.

Minor app #1	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?		

Minor app #2	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?		

Minor app #3	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?		

Baker System	Veterans Assistance Discharge System (VADS)
Dental Records Manager	VBA Training Academy
Sidexis	Veterans Service Network (VETSNET)
Priv Plus	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
Mental Health Assistant	BIRLS
Telecare Record Manager	Centralized Accounts Receivable System (CARS)
Omicell	Compensation & Pension (C&P)
Powerscribe Dictation System	Corporate Database
EndoSoft	Control of Veterans Records (COVERS)
Compensation and Pension (C&P)	Data Warehouse
Montgomery GI Bill	INS - BIRLS
Vocational Rehabilitation & Employment (VR&E) CH 31	Mobilization
Post Vietnam Era educational Program (VEAP) CH 32	Master Veterans Record (MVR)
Spinal Bifida Program Ch 18	BDN Payment History
C&P Payment System	
Survivors and Dependents Education Assistance CH 35	
Reinstatement Entitlement Program for Survivors (REAPS)	
Educational Assistance for Members of the Selected Reserve Program CH 1606	
Reserve Educational Assistance Program CH 1607	
Compensation & Pension Training Website	
Web-Enabled Approval Management System (WEAMS)	
FOCAS	
Work Study Management System (WSMS)	
Benefits Delivery Network (BDN)	
Personnel and Accounting Integrated Data and Fee Basis (PAID)	
Personnel Information Exchange System (PIES)	
Rating Board Automation 2000 (RBA2000)	
SHARE	
Service Member Records Tracking System	

(FY 2010) PIA: VISTA Minor Applications

Explain what minor application that are associated with your installation? (Check all that apply)

Yes	ACCOUNTS RECEIVABLE	Yes	DRUG ACCOUNTABILITY	INPATIENT MEDICATIONS	Yes
	ADP PLANNING (PLANMAN)	Yes	DSS EXTRACTS	INTAKE/OUTPUT	Yes
Yes	ADVERSE REACTION TRACKING		EDUCATION TRACKING	Yes	INTEGRATED BILLING
Yes	ASISTS	Yes	EEO COMPLAINT TRACKING	Yes	INTEGRATED PATIENT FUNDS
Yes	AUTHORIZATION/SUBSCRIPTION	Yes	ELECTRONIC SIGNATURE	Yes	INTERIM MANAGEMENT SUPPORT
Yes	AUTO REPLENISHMENT/WARD STOCK	Yes	ENGINEERING	Yes	KERNEL
Yes	AUTOMATED INFO COLLECTION SYS	Yes	ENROLLMENT APPLICATION SYSTEM	Yes	KIDS
Yes	AUTOMATED LAB INSTRUMENTS	Yes	EQUIPMENT/TURN-IN REQUEST	Yes	LAB SERVICE
Yes	AUTOMATED MED INFO EXCHANGE	Yes	EVENT CAPTURE	LETTERMAN	Yes
Yes	BAR CODE MED ADMIN	Yes	EVENT DRIVEN REPORTING	Yes	LEXICON UTILITY
Yes	BED CONTROL	Yes	EXTENSIBLE EDITOR	Yes	LIBRARY
Yes	BENEFICIARY TRAVEL	Yes	EXTERNAL PEER REVIEW	Yes	LIST MANAGER
	CAPACITY MANAGEMENT - RUM	Yes	FEE BASIS	Yes	MAILMAN
	CAPRI	Yes	FUNCTIONAL INDEPENDENCE	Yes	MASTER PATIENT INDEX VISTA
	CAPACITY MANAGEMENT TOOLS	Yes	GEN. MED. REC. - GENERATOR	Yes	MCCR NATIONAL DATABASE
	CARE MANAGEMENT	Yes	GEN. MED. REC. - I/O	Yes	MEDICINE
Yes	CLINICAL CASE REGISTRIES	Yes	GEN. MED. REC. - VITALS	Yes	MENTAL HEALTH
Yes	CLINICAL INFO RESOURCE NETWORK	Yes	GENERIC CODE SHEET	MICOM	Yes
Yes	CLINICAL MONITORING SYSTEM		GRECC	Yes	MINIMAL PATIENT DATASET
Yes	CLINICAL PROCEDURES	Yes	HEALTH DATA & INFORMATICS	Yes	MYHEALTHVET
Yes	CLINICAL REMINDERS	Yes	HEALTH LEVEL SEVEN	Missing Patient Reg (Original)	Yes
Yes	CMOP	Yes	HEALTH SUMMARY	Yes	NATIONAL DRUG FILE
Yes	CONSULT/REQUEST TRACKING	Yes	HINQ	Yes	NATIONAL LABORATORY TEST
Yes	CONTROLLED SUBSTANCES	Yes	HOSPITAL BASED HOME CARE	Yes	NDBI
Yes	CPT/HCPCS CODES		ICR - IMMUNOLOGY CASE REGISTRY	Yes	NETWORK HEALTH EXCHANGE

Yes CREDENTIALS TRACKING	Yes IFCAP	NOIS	
Yes DENTAL	Yes IMAGING	Yes NURSING SERVICE	Yes
Yes DIETETICS	Yes INCIDENT REPORTING	Yes OCCURRENCE SCREEN	Yes
Yes DISCHARGE SUMMARY	Yes INCOME VERIFICATION MATCH	Yes ONCOLOGY	
Yes DRG GROUPER	Yes INCOMPLETE RECORDS TRACKING	Yes ORDER ENTRY/RESULTS REPORTING	Yes

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
Bed Board Management System		
<input checked="" type="checkbox"/> YES Is PII collected by this min or application?		
Does this minor application store PII?		
<input checked="" type="checkbox"/> YES If yes, where?		Dedicated Server
Who has access to this data?		Limited IT Personnel, Limited Clinical Staff,

Minor app #1

Name	Description	Comments
Automated Access Request (AAR)		
<input checked="" type="checkbox"/> YES Is PII collected by this min or application?		
Does this minor application store PII?		
<input checked="" type="checkbox"/> YES If yes, where?		Vista
Who has access to this data?		HR Personnel

Minor app #2

Name	Description	Comments
Health Summary Contingency		
<input checked="" type="checkbox"/> YES Is PII collected by this min or application?		
Does this minor application store PII?		
<input checked="" type="checkbox"/> YES If yes, where?		Dedicated Contingency PCs
Who has access to this data?		IT Personnel, Limited Clinical Staff

Minor app #3

OUTPATIENT PHARMACY	Yes	SOCIAL WORK
PAID	Yes	SPINAL CORD DYSFUNCTION
PATCH MODULE	Yes	SURGERY
PATIENT DATA EXCHANGE	Yes	SURVEY GENERATOR
PATIENT FEEDBACK	Yes	TEXT INTEGRATION UTILITIES
PATIENT REPRESENTATIVE	Yes	TOOLKIT
PCE PATIENT CARE ENCOUNTER		UNWINDER
PCE PATIENT/IHS SUBSET	Yes	UTILIZATION MANAGEMENT ROLLUP
PHARMACY BENEFITS MANAGEMENT		UTILIZATION REVIEW
PHARMACY DATA MANAGEMENT	Yes	VA CERTIFIED COMPONENTS - DSSI
PHARMACY NATIONAL DATABASE	Yes	VA FILEMAN
PHARMACY PRESCRIPTION PRACTICE	Yes	VBECS
POLICE & SECURITY	Yes	VDEF
PROBLEM LIST	Yes	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES	Yes	VHS&RA ADP TRACKING SYSTEM
PROSTHETICS	Yes	VISIT TRACKING
QUALITY ASSURANCE INTEGRATION	Yes	VISTALINK
QUALITY IMPROVEMENT CHECKLIST	Yes	VISTALINK SECURITY
QUASAR	Yes	VISUAL IMPAIRMENT SERVICE TEAM ANRV
RADIOLOGY/NUCLEAR MEDICINE	Yes	VOLUNTARY TIMEKEEPING
RECORD TRACKING		VOLUNTARY TIMEKEEPING NATIONAL
REGISTRATION	Yes	WOMEN'S HEALTH
RELEASE OF INFORMATION - DSSI		CARE TRACKER
REMOTE ORDER/ENTRY SYSTEM		
RPC BROKER		

RUN TIME LIBRARY
SAGG
SCHEDULING

SECURITY SUITE UTILITY PACK

SHIFT CHANGE HANDOFF
TOOL

(FY 2010) PIA: Minor Applications

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

Minor app #1	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?			

Minor app #2	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?			

Minor app #3	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 2010) PIA: Final Signatures

Facility Name: Charlie Norwood VA Medial Center (509)

Title:	Name:	Phone:	Email:
Privacy Officer:	Shawana Burch	(706) 733-0188	shawana.burch@va.gov
Information Security Officer:	Sue Heath	(706) 481-6743	sue.Heath@va.gov
Chief Information Officer:	Gerald Crawford	(706) 481-6750	Gerald.Crawford@va.gov
Person Completing Document:	Shawana Burch	(706) 733-0188	shawana.burch@va.gov
System / Application / Program Manager:	Rebecca Swords	(706) 481-6775	Rebecca.Swords@va.gov

Date of Report: 3/29/2010
OMB Unique Project Identifier: 029-00-01-11-01-1180-00
Project Name: REGION3>VHA>VISN 7> Charlie Norwood VAMC> VistA Legacy