

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 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: Region 3>VHA.VISN8>WPBVAMC>VISTA

OMB Unique System / Application / Program Identifier (AKA: UPID #): **029-00-01-11-01-1180-00**

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 2500 FTE) necessary to operate the system. VistA-Legacy is a client-server system. It links the facility computer network to over

Description of System / Application / Program: 100 applications and databases.

Facility Name: WPB VAMC

Title:	Name:	Phone:	Email:
Privacy Officer:	Mary Beth Hudak	561-422-7736	mary.hudak@va.gov
Information Security Officer:	Umila Garib	561-422-8214	Umila.Garib@va.gov
Chief Information Officer:	Karen Gabaldon	561-422-6800	Karen.Gabaldon@va.gov
Person Completing Document:	Mary Beth Hudak	561-422-7736	mary.hudak@va.gov
Other Titles:	Thiem N. Tieu	(561) 422-7516	Thiem.Tieu@va.gov
Facility Information Security Officer	Umila Garib	561-422-8214	Umila.Garib@va.gov

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)

04/2009

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. 06/1995

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): 07/2009

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)

(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, 24VA19

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)	Paper	The most common data types that are captured and accessed on a regular basis by authorized individuals are first and last name, middle initial, DOB, SSN, and address. This patient information falls into two classes: administrative and clinical. Clinical information is used to diagnose, prescribe treatment and follow clinically the patient through his/her health care encounters. Administrative data is used to identify the veteran (SSN), correspond to/from (name and address), and determine eligibility (patient administrative info + SSA and IRS data), enter NOK and emergency contact information and collect insurance information.	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	Paper	Dependent Data is utilized to determine eligibility for VA benefits. In addition, NOK and emergency contact information is often a dependent of the veteran and this data is used in case of emergency or need during the patient's episode of care.	Written	Written
Service Information	Electronic/File Transfer	Military Service Information (Branch of service, discharge date, discharge type, service connection r	Verbally	Written
Medical Information	Verbal	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, 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.	Verbally	Written
Criminal Record Information	Electronic/File Transfer	Specific information is not input into the Vista system but the fugitive felon program includes a flag on the patient file identifying the need to contact the VA police.	Verbally	Written

Guardian Information	Verbal	Guardian information is often flagged in the medical record to ensure the timely and appropriate notification during healthcare decision making from provider/patient/guardian.	Written	Written
Education Information	N/A	N/A		
Benefit Information	Electronic/File Transfer	VIS, HINQ, VERA, KLF, used to verify service dates, eligibility, SSN, etc.	Written	Written
Other (Explain)	Paper	Next-of-kin information and emergency contact information, such as name and telephone number, is collected from the veteran to use to contact other individuals in case of an emergency. In addition insurance and employment information is available on the veteran for use in billing for care. Religious information is collected to provide for spiritual needs if requested by the veteran.	Written	Written

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	VA Files / Databases (Identify file)	Mandatory	VBA
Medical Information	Yes	Veteran	Mandatory	
Criminal Record Information	Yes	State Agency (Identify)	Mandatory	Fugitive Felon
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	VBA	No	Patient information re: treatment and demographic for benefits determination	Both PII & PHI	VHA Handbook 1605.1, MCM 136H-116
Other Veteran Organization	Office of Regional Counsel	No	Tort Claims, legal processes	Both PII & PHI	national BAA
Other Federal Government Agency	Congressional Offices	No	Appointment dates, treatment, medical documentation, bills, co-pays	Both PII & PHI	VHA Handbook 1605.1, MCM 136H-116
State Government Agency	CDC	No	HIV Results	Both PII & PHI	VHA Handbook 1605.1, MCM 136H-116
Local Government Agency		No			
Research Entity	n/a	No		N/A	
Other Project / System					
Other Project / System					
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? Yes

if yes, please check all that apply:

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

Describe process for authorizing access to this data.
Answer:

Access is authorized to only VA employees, contractors with a BAA, students, and volunteers who completed a background check and the mandatory privacy and cyber security training

(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 manually by staff. Additionally, Vista database has specific fields; if there is no field created, the data will not be stored.

How is data checked for completeness?

Answer: The database has required field that need to be answered. If the user did not enter any data in those fields, he/she would not be able to submit the data. Also, the data is reviewed by the user and compared to paper forms.

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

Answer: Vista database uses the process "journaling" that updates the database and the shadow server at the same time. There are also periodic reviews by supervisors and administrative staff update the information with each application of care.

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

Answer: It is verified by the new patches for Vista, checked for check-sum, which shows the accuracy of the data. New data is compared with previous data and 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: 75 years which is in accordance with the VA Record Control Schedule (RCS) 10-1

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

Answer: Clinical information is retained in accordance with VA Records Control Schedule (RCS) 10-1.

Demographic information is updated as applications for care are submitted and retained in accordance with VA RCS 10-1

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

Answer: Electronic final version of the patient medical record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA RCS 10-1, Item XLIII, 2.b. At the present time, Vista Imaging retains all images. VHA Handbook 1907.1 (Section 6) and VA RCS 10-1 provide more general guidance.

Where are these procedures documented?

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

How are data retention procedures enforced?

Answer: VA RCS 10-1: Records management responsibilities are assigned to the Records Control Officer for the facility. The RCO is responsible for developing policies and procedures for effective and efficient records management throughout the West Palm Beach VAMC. In addition, the RCO, acts as the liaison between VHA and National Archives and Records Administration (NARA) on issues pertaining to records management practices and procedures. All VHA employees are responsible to ensure that records are created, maintained, and 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

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? 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: Per OMB guidance, implementing requirements of the Federal Information Security Management Act of 2006.

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"/> Hardware Failure |
| <input type="checkbox"/> Chemical/Biological Contamination | <input checked="" type="checkbox"/> Malicious Code |
| <input type="checkbox"/> Blackmail | <input checked="" type="checkbox"/> Computer Misuse |
| <input checked="" type="checkbox"/> Bomb Threats | <input checked="" type="checkbox"/> Power Loss |
| <input type="checkbox"/> Cold/Frost/Snow | <input type="checkbox"/> Sabotage/Terrorism |
| <input checked="" type="checkbox"/> Communications Loss | <input checked="" type="checkbox"/> Storms/Hurricanes |
| <input checked="" type="checkbox"/> Computer Intrusion | <input type="checkbox"/> Substance Abuse |
| <input checked="" type="checkbox"/> Data Destruction | <input type="checkbox"/> Theft of Assets |
| <input checked="" type="checkbox"/> Data Disclosure | <input checked="" type="checkbox"/> Theft of Data |
| <input checked="" type="checkbox"/> Data Integrity Loss | <input type="checkbox"/> Vandalism/Rioting |
| <input checked="" 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 type="checkbox"/> Eavesdropping/Interception | <input checked="" type="checkbox"/> Identity Theft |
| <input checked="" type="checkbox"/> Fire (False Alarm, Major, and Minor) | <input type="checkbox"/> Fraud/Embezzlement |
| <input checked="" 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 checked="" type="checkbox"/> Media Protection |
| <input checked="" type="checkbox"/> Personnel Security | |
| <input checked="" type="checkbox"/> Certification and Accreditation Security Assessments | |

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: Keeping existing procedures

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?

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 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 Veterans Assistance Discharge System (VADS)	Education Training Website VR&E Training Website VA Reserve Educational Assistance Program	Appraisal System Web Electronic Lender Identification	Baker System Dental Records Manager	Veterans Assistance Discharge System (VADS) VBA Training Academy
LGY Processing	Web Automated Verification of Enrollment Right Now Web VA Online Certification of Enrollment (VA-ONCE)	CONDO PUD Builder Centralized Property Tracking System Electronic Appraisal System	Sidexis Priv Plus Mental Health Asisstant	Veterans Service Network (VETSNET) Waco Indianapolis, Newark, Roanoke, Seattle (WINRS) BIRLS Centralized Accounts Receivable System (CARS)
Loan Service and Claims LGY Home Loans	Automated Folder Processing System (AFPS) Personal Computer Generated Letters (PCGL) Personnel Information Exchange System (PIES) Rating Board Automation 2000 (RBA2000)	Web LGY Access Manager SAHSHA	Telecare Record Manager Omnicell Powerscribe Dictation System	Compensation & Pension (C&P) Corporate Database Control of Veterans Records (COVERS)
Search Participant Profile (SPP) Control of Veterans Records (COVERS)		VBA Data Warehouse Distribution of Operational Resources (DOOR)	EndoSoft Compensation and Pension (C&P)	Data Warehouse
SHARE Modern Awards Process Development (MAP-D) Rating Board Automation 2000 (RBA2000)	SHARE	Enterprise Wireless Messaging System (Blackberry) VBA Enterprise Messaging System	Montgomery GI Bill Vocational Rehabilitation & Employment (VR&E) CH 31 Post Vietnam Era educational Program (VEAP) CH 32	INS - BIRLS Mobilization
State of Case/Supplemental (SOC/SSOC)	State Benefits Reference System Training and Performance Support System (TPSS) Veterans Appeals Control and Locator System (VACOLS) Veterans On-Line Applications (VONAPP)	LGY Centralized Fax System Review of Quality (ROQ) Automated Sales Reporting (ASR)	Spinal Bifida Program Ch 18 C&P Payment System	Master Veterans Record (MVR) BDN Payment History
Awards Financial and Accounting System (FAS)				
Eligibility Verification Report (EVR) Automated Medical Information System (AMIS)290				

Web Automated Reference Material System (WARMS)	Automated Medical Information Exchange II (AIME II)	Electronic Card System (ECS)	Survivors and Dependents Education Assistance CH 35
Automated Standardized Performance Elements Nationwide (ASPEN)	Committee on Waivers and Compromises (COWC)	Electronic Payroll Deduction (EPD)	Reinstatement Entitlement Program for Survivors (REAPS)
Inquiry Routing Information System (IRIS)	Common Security User Manager (CSUM)	Financial Management Information System (FMI)	Educational Assistance for Members of the Selected Reserve Program CH 1606
National Silent Monitoring (NSM)	Compensation and Pension (C&P) Record Interchange (CAPRI)	Purchase Order Management System (POMS)	Reserve Educational Assistance Program CH 1607
Web Service Medical Records (WebSMR)	Control of Veterans Records (COVERS)	Veterans Canteen Web	Compensation & Pension Training Website
Systematic Technical Accuracy Review (STAR)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)	Inventory Management System (IMS)	Web-Enabled Approval Management System (WEAMS)
Fiduciary STAR Case Review	Fiduciary Beneficiary System (FBS)	Synquest	FOCAS
Veterans Exam Request Info System (VERIS)	Hearing Officer Letters and Reports System (HOLAR)	RAI/MDS	Work Study Management System (WSMS)
Web Automated Folder Processing System (WAFPS)	Inforce	ASSISTS	Benefits Delivery Network (BDN)
Courseware Delivery System (CDS)	Awards	MUSE	Personnel and Accounting Integrated Data and Fee Basis (PAID)
Electronic Performance Support System (EPSS)	Actuarial	Bbraun (CP Hemo)	Personnel Information Exchange System (PIES)
Veterans Service Representative (VSR) Advisor	Insurance Self Service	VIC	Rating Board Automation 2000 (RBA2000)
Loan Guaranty Training Website	Insurance Unclaimed Liabilities	BCMA Contingency Machines	SHARE
C&P Training Website	Insurance Online	Script Pro	Service Member Records Tracking System

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
<input type="checkbox"/> Is PII collected by this min or application?		
<input type="checkbox"/> Does this minor application store PII?		
If yes, where?		
Who has access to this data?		

Minor app #1

Name	Description	Comments
<input type="checkbox"/> Is PII collected by this min or application?		
<input type="checkbox"/> Does this minor application store PII?		
If yes, where?		
Who has access to this data?		

Minor app #2

Name	Description	Comments
<input type="checkbox"/> Is PII collected by this min or application?		
<input type="checkbox"/> Does this minor application store PII?		
If yes, where?		
Who has access to this data?		

Minor app #3

(FY 2010) PIA: VISTA Minor Applications

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

X	ACCOUNTS RECEIVABLE	X	DRUG ACCOUNTABILITY	X	INPATIENT MEDICATIONS	X	OUTPATIENT PHARMACY	X	SOCIAL WORK
	ADP PLANNING (PLANMAN)	X	DSS EXTRACTS	X	INTAKE/OUTPUT	X	PAID	X	SPINAL CORD DYSFUNCTION
X	ADVERSE REACTION TRACKING	X	EDUCATION TRACKING	X	INTEGRATED BILLING	X	PATCH MODULE	X	SURGERY
X	ASISTS	X	EEO COMPLAINT TRACKING	X	INTEGRATED PATIENT FUNDS	X	PATIENT DATA EXCHANGE	X	SURVEY GENERATOR
X	AUTHORIZATION/SUBSCRIPTION	X	ELECTRONIC SIGNATURE	X	INTERIM MANAGEMENT SUPPORT	X	PATIENT FEEDBACK	X	TEXT INTEGRATION UTILITIES
X	AUTO REPLENISHMENT/WARD STOCK	X	ENGINEERING	X	KERNEL	X	PATIENT REPRESENTATIVE	X	TOOLKIT
X	AUTOMATED INFO COLLECTION SYS	X	ENROLLMENT APPLICATION SYSTEM	X	KIDS	X	PCE PATIENT CARE ENCOUNTER	X	UNWINDER
X	AUTOMATED LAB INSTRUMENTS	X	EQUIPMENT/TURN-IN REQUEST	X	LAB SERVICE	X	PCE PATIENT/IHS SUBSET	X	UTILIZATION MANAGEMENT ROLLUP
X	AUTOMATED MED INFO EXCHANGE	X	EVENT CAPTURE	X	LETTERMAN	X	PHARMACY BENEFITS MANAGEMENT	X	UTILIZATION REVIEW
X	BAR CODE MED ADMIN	X	EVENT DRIVEN REPORTING	X	LEXICON UTILITY	X	PHARMACY DATA MANAGEMENT	X	VA CERTIFIED COMPONENTS - DSSI
X	BED CONTROL	X	EXTENSIBLE EDITOR	X	LIBRARY	X	PHARMACY NATIONAL DATABASE	X	VA FILEMAN
X	BENEFICIARY TRAVEL	X	EXTERNAL PEER REVIEW	X	LIST MANAGER	X	PHARMACY PRESCRIPTION PRACTICE	X	VBECs
X	CAPRI	X	FUNCTIONAL INDEPENDENCE	X	MAILMAN	X	POLICE & SECURITY	X	VDEF
X	CAPRI	X	FUNCTIONAL INDEPENDENCE	X	MASTER PATIENT INDEX VISTA	X	PROBLEM LIST	X	VENDOR - DOCUMENT STORAGE SYS

	CAPACITY MANAGEMENT TOOLS	X	GEN. MED. REC. - GENERATOR	X	MCCR NATIONAL DATABASE	X	PROGRESS NOTES	VHS&RA ADP TRACKING SYSTEM
X	CARE MANAGEMENT	X	GEN. MED. REC. - I/O	X	MEDICINE	X	PROSTHETICS	X VISIT TRACKING
X	CLINICAL CASE REGISTRIES	X	GEN. MED. REC. - VITALS	X	MENTAL HEALTH	X	QUALITY ASSURANCE INTEGRATION	X VISTALINK
X	CLINICAL INFO RESOURCE NETWORK	X	GENERIC CODE SHEET	X	MICOM	X	QUALITY IMPROVEMENT CHECKLIST	X VISTALINK SECURITY
X	CLINICAL MONITORING SYSTEM		GRECC	X	MINIMAL PATIENT DATASET	X	QUASAR	X VISUAL IMPAIRMENT SERVICE TEAM ANRV
X	CLINICAL PROCEDURES	X	HEALTH DATA & INFORMATICS		MYHEALTHEVET	X	RADIOLOGY/NUCLEAR MEDICINE	X VOLUNTARY TIMEKEEPING
X	CLINICAL REMINDERS		HEALTH LEVEL SEVEN	X	Missing Patient Reg (Original) A4EL	X	RECORD TRACKING	X VOLUNTARY TIMEKEEPING NATIONAL
X	CMOP	X	HEALTH SUMMARY	X	NATIONAL DRUG FILE	X	REGISTRATION	X WOMEN'S HEALTH
X	CONSULT/REQUEST TRACKING	X	HINQ	X	NATIONAL LABORATORY TEST		RELEASE OF INFORMATION - DSSI	CARE TRACKER
X	CONTROLLED SUBSTANCES	X	HOSPITAL BASED HOME CARE		NDBI	X	REMOTE ORDER/ENTRY SYSTEM	
X	CPT/HCPCS CODES	X	ICR - IMMUNOLOGY CASE REGISTRY		NETWORK HEALTH EXCHANGE	X	RPC BROKER	
X	CREDENTIALS TRACKING	X	IFCAP	X	NOIS		RUN TIME LIBRARY	
	DENTAL		IMAGING		NURSING SERVICE		SAGG	
X	DIETETICS	X	INCIDENT REPORTING	X	OCCURRENCE SCREEN	X	SCHEDULING	
X	DISCHARGE SUMMARY	X	INCOME VERIFICATION MATCH	X	ONCOLOGY		SECURITY SUITE UTILITY PACK	
X	DRG GROUPER	X	INCOMPLETE RECORDS TRACKING	X	ORDER ENTRY/RESULTS REPORTING	X	SHIFT CHANGE HANDOFF TOOL	

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?

Minor app #1

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?

Minor app #2

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?

Minor app #3

Does this minor application store PII?

If yes, where?

Who has access to this data?

(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
		<input type="checkbox"/>	Is PII collected by this min or application?		
		<input type="checkbox"/>	Does this minor application store PII?		
			If yes, where?		
		Who has access to this data?			

Minor app #2	Name		Description		Comments
		<input type="checkbox"/>	Is PII collected by this min or application?		
		<input type="checkbox"/>	Does this minor application store PII?		
			If yes, where?		
		Who has access to this data?			

Minor app #3	Name		Description		Comments
		<input type="checkbox"/>	Is PII collected by this min or application?		
		<input type="checkbox"/>	Does this minor application store PII?		
			If yes, where?		
		Who has access to this data?			

(FY 2010) PIA: Final Signatures

Facility Name: WPB VAMC

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

Privacy Officer:	Mary Beth Hudak	561-422-7736	mary.hudak@va.gov
------------------	-----------------	--------------	-------------------



Information Security Officer:	Umila Garib	561-422-8214	Umila.Garib@va.gov
-------------------------------	-------------	--------------	--------------------



Chief Information Officer:	Karen Gabaldon	561-422-6800	Karen.Gabaldon@va.gov
----------------------------	----------------	--------------	-----------------------



Person Completing Document:	Mary Beth Hudak	561-422-7736	mary.hudak@va.gov
-----------------------------	-----------------	--------------	-------------------



System / Application / Program Manager:	Thiem N. Tieu	(561) 422-7516	Thiem.Tieu@va.gov
---	---------------	----------------	-------------------



Date of Report: 11/4/2009

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

Project Name Region
3>VHA.VISN8>WPBVAMC>VISTA