

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://vaww.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 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

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 >VISN 8>WPB VAMC>PBX

OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-02-00-01-1120-00

Each VA medical center uses the Network (PBX) as a General Support System, supporting mission-critical and other systems necessary to conduct day-to-day operations within the Veterans Health Administration. Applications and devices within the PBX support numerous areas, including medical imaging, supply management, decision

Description of System / Application / Program: support, medical research, and education.

Facility Name: West Palm Beach 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:	David Shoaff	561-422-5520	David.Shoaff@NVUT.com
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:

07/2012

What specific legal authorities authorize this program or system: N/A

What is the expected number of individuals that will have their PII stored in this system: N/A

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. 6 yrs

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): 04/2009

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?

No

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

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

Does the System of Records Notice require modification or updating?

(Please Select Yes/No)

Is PII collected by paper methods?

No

Is PII collected by verbal methods?

No

Is PII collected by automated methods?

No

Is a Privacy notice provided?

No

Proximity and Timing: Is the privacy notice provided at the time of data collection?

No

Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

No

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

No

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

No

(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)	N/A		Verbally	
Family Relation (spouse, children, parents, grandparents, etc)	N/A		Written	
Service Information	N/A		Verbally	
Medical Information	N/A			
Criminal Record Information				
Guardian Information	N/A			
Education Information	N/A			
Benefit Information	N/A			
Other (Explain)	N/A			

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)	No			
Family Relation (spouse, children, parents, grandparents, etc)	No			
Service Information	No			
Medical Information	No			
Criminal Record Information	No			
Guardian Information	No			
Education Information	No			
Benefit Information	No			
Other (Explain)	No			
Other (Explain)	No			
Other (Explain)	No			

(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		No		N/A	
Other Veteran Organization		No		N/A	
Other Federal Government Agency		No		N/A	
State Government Agency		No		N/A	
Local Government Agency		No		N/A	
Research Entity		No		N/A	
Other Project / System		No		N/A	
Other Project / System		No		N/A	
Other Project / System		No		N/A	

(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? No

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:

How is data checked for completeness?

Answer:

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

Answer:

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

Answer:

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:

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

Answer:

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

Answer:

Where are these procedures documented?

Answer:

How are data retention procedures enforced?

Answer:

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

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:

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

- | | |
|---|--|
| <input type="checkbox"/> Air Conditioning Failure | <input type="checkbox"/> Hardware Failure |
| <input type="checkbox"/> Chemical/Biological Contamination | <input 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 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 type="checkbox"/> Errors (Configuration and Data Entry) |
| <input type="checkbox"/> Earthquakes | <input type="checkbox"/> Burglary/Break In/Robbery |
| <input type="checkbox"/> Eavesdropping/Interception | <input 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 type="checkbox"/> Risk Management | <input type="checkbox"/> Audit and Accountability |
| <input type="checkbox"/> Access Control | <input type="checkbox"/> Configuration Management |
| <input type="checkbox"/> Awareness and Training | <input type="checkbox"/> Identification and Authentication |
| <input type="checkbox"/> Contingency Planning | <input type="checkbox"/> Incident Response |
| <input type="checkbox"/> Physical and Environmental Protection | <input type="checkbox"/> Media Protection |
| <input type="checkbox"/> Personnel Security | |
| <input 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:

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?

FALSE

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

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

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 #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

(FY 2010) PIA: VISTA Minor Applications

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

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

CAPACITY MANAGEMENT TOOLS	GEN. MED. REC. - GENERATOR	MCCR NATIONAL DATABASE	PROGRESS NOTES	VHS&RA ADP TRACKING SYSTEM
CARE MANAGEMENT	GEN. MED. REC. - I/O	MEDICINE	PROSTHETICS	VISIT TRACKING
CLINICAL CASE REGISTRIES	GEN. MED. REC. - VITALS	MENTAL HEALTH	QUALITY ASSURANCE INTEGRATION	VISTALINK
CLINICAL INFO RESOURCE NETWORK	GENERIC CODE SHEET	MICOM	QUALITY IMPROVEMENT CHECKLIST	VISTALINK SECURITY
CLINICAL MONITORING SYSTEM	GRECC	MINIMAL PATIENT DATASET	QUASAR	VISUAL IMPAIRMENT SERVICE TEAM ANRV
CLINICAL PROCEDURES	HEALTH DATA & INFORMATICS	MYHEALTHVET	RADIOLOGY/NUCLEAR MEDICINE	VOLUNTARY TIMEKEEPING
CLINICAL REMINDERS	HEALTH LEVEL SEVEN	Missing Patient Reg (Original) A4EL	RECORD TRACKING	VOLUNTARY TIMEKEEPING NATIONAL
CMOP	HEALTH SUMMARY	NATIONAL DRUG FILE	REGISTRATION	WOMEN'S HEALTH
CONSULT/REQUEST TRACKING	HINQ	NATIONAL LABORATORY TEST	RELEASE OF INFORMATION - DSSI	CARE TRACKER
CONTROLLED SUBSTANCES	HOSPITAL BASED HOME CARE	NDBI	REMOTE ORDER/ENTRY SYSTEM	
CPT/HCPCS CODES	ICR - IMMUNOLOGY CASE REGISTRY	NETWORK HEALTH EXCHANGE	RPC BROKER	
CREDENTIALS TRACKING	IFCAP	NOIS	RUN TIME LIBRARY	
DENTAL	IMAGING	NURSING SERVICE	SAGG	
DIETETICS	INCIDENT REPORTING	OCCURRENCE SCREEN	SCHEDULING	
DISCHARGE SUMMARY	INCOME VERIFICATION MATCH	ONCOLOGY	SECURITY SUITE UTILITY PACK	
DRG GROUPER	INCOMPLETE RECORDS TRACKING	ORDER ENTRY/RESULTS REPORTING	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
<input type="checkbox"/> Is PII collected by this min or application?		
Minor app #1	<input type="checkbox"/> Does this minor application store PII?	
	<input type="checkbox"/> If yes, where?	
	<input type="text"/> Who has access to this data?	

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

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

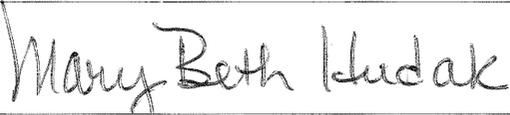
Minor app #3	Name		Description		Comments
		<input type="checkbox"/>	Is PII collected by this min or application?		
		<input type="checkbox"/>	Does this minor application store PII?		
			If yes, where?		
		Who has access to this data?			

(FY 2010) PIA: Final Signatures

Facility Name: West Palm Beach VAMC

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

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



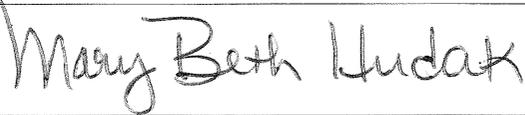
Information Security Officer:	Umila Garib	561-422-8214	Umila.Garib@va.gov
-------------------------------	-------------	--------------	--------------------



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:	David Shoaff	561-422-5520	David Shoaff@NVUT.com
---	--------------	--------------	-----------------------



Date of Report: 4/1/2009

OMB Unique Project Identifier 029-00-02-00-01-1120-00

Project Name Region 3 >VISN 8>WPB VAMC>PBX