

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: Home Telehealth

OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-01-11-01-1186-00-105-03-001-00

Collects patient data from a remote location to used by the Care Coordinators to evaluate the patients

Description of System / Application / Program: condition.

Facility Name: Silver Spring IOFO

Title:	Name:	Phone:	Email:
Privacy Officer:	Garnett Best	202-461-7474	Garnett.Best@va.gov
Information Security Officer:	Paula Pinckney	301-734-0438	Paula.Pinckney@va.gov
Chief Information Officer:	Joe Gibbons	518-449-0618	Joe.Gibbons@va.gov
Person Completing Document:	Bernard Brauner	301-734-0369	Bernard.Brauner@va.gov

Other Titles:

Other Titles:

Other Titles:

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

08/2008

Date Approval To Operate Expires:

12/2011

What specific legal authorities authorize this program or system:

Under Secretary for Health

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

100000

Identify what stage the System / Application / Program is at:

Implementation

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. 08/2008

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):

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:

Veterans Health Information Systems
Technology (VISTA)

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

http://www.rms.oit.va.gov/SOR_Records/79VA19.asp [Records/24VA19.asp](http://www.rms.oit.va.gov/SOR_Records/24VA19.asp)

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?

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)	Verbal	The information will be used only by the VA for medical evaluation purposes.	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	N/A			
Service Information	N/A			
Medical Information	Web Data Storage Device	It will be used by the Care Coordinators	Written	Written
Criminal Record Information	Paper	For VA use only	Written	Written
Guardian Information	Paper	For VA use only	Written	Written
Education Information	Verbal	For VA use only	Written	Written
Benefit Information	Verbal	For VA use only	Written	Written
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	Voluntary	
Family Relation (spouse, children, parents, grandparents, etc)	No			
Service Information	No			
Medical Information	Yes	Veteran	Voluntary	
Criminal Record Information	No			
Guardian Information	No			
Education Information	No			
Benefit Information	No			
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	MPI	Yes	Name change, DOB,ssn change	N/A	VA Policy
Other Veteran Organization	HDR	Yes	Medical	PII	VA Policy
Other Federal Government Agency		No			
State Government Agency		No			
Local Government Agency		No			
Research Entity		No			
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? 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) 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:

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 type="checkbox"/> Malicious Code |
| <input type="checkbox"/> Blackmail | <input type="checkbox"/> Computer Misuse |
| <input type="checkbox"/> Bomb Threats | <input checked="" 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 checked="" type="checkbox"/> Audit and Accountability |
| <input checked="" type="checkbox"/> Access Control | <input checked="" type="checkbox"/> Configuration Management |
| <input type="checkbox"/> Awareness and Training | <input checked="" type="checkbox"/> Identification and Authentication |
| <input type="checkbox"/> Contingency Planning | <input 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)

PIA: PIA Assessment

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

Answer: We review the security controls of the system.

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

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? If yes, where?	
	<input type="checkbox"/> 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? If yes, where?	
	<input type="checkbox"/> 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? If yes, where?	
	<input type="checkbox"/> Who has access to this data?	

Baker System	Veterans Assistance Discharge System (VADS)
Dental Records Manager	VBA Training Academy
Sidexis	Veterans Service Network (VETSNET) Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
Priv Plus Mental Health Assistant	BIRLS Centralized Accounts Receivable System (CARS)
Telecare Record Manager	
Omnicell	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 Vocational Rehabilitation & Employment (VR&E) CH 31 Post Vietnam Era educational Program (VEAP) CH 32	INS - BIRLS Mobilization 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)

ACCOUNTS RECEIVABLE	DRUG ACCOUNTABILITY	INPATIENT MEDICATIONS
ADP PLANNING (PLANMAN) ADVERSE REACTION TRACKING ASISTS	DSS EXTRACTS EDUCATION TRACKING EEO COMPLAINT TRACKING	INTAKE/OUTPUT INTEGRATED BILLING INTEGRATED PATIENT FUNDS
AUTHORIZATION/SUBSCRIPTION	ELECTRONIC SIGNATURE	INTERIM MANAGEMENT SUPPORT
AUTO REPLENISHMENT/WARD STOCK	ENGINEERING	KERNEL
AUTOMATED INFO COLLECTION SYS	ENROLLMENT APPLICATION SYSTEM	KIDS
AUTOMATED LAB INSTRUMENTS	EQUIPMENT/TURN-IN REQUEST	LAB SERVICE
AUTOMATED MED INFO EXCHANGE	EVENT CAPTURE	LETTERMAN
BAR CODE MED ADMIN	EVENT DRIVEN REPORTING	LEXICON UTILITY
BED CONTROL	EXTENSIBLE EDITOR	LIBRARY
BENEFICIARY TRAVEL	EXTERNAL PEER REVIEW	LIST MANAGER
CAPACITY MANAGEMENT - RUM	FEE BASIS	MAILMAN
CAPRI	FUNCTIONAL INDEPENDENCE	MASTER PATIENT INDEX VISTA
CAPACITY MANAGEMENT TOOLS	GEN. MED. REC. - GENERATOR	MCCR NATIONAL DATABASE
CARE MANAGEMENT CLINICAL CASE REGISTRIES	GEN. MED. REC. - I/O GEN. MED. REC. - VITALS	MEDICINE MENTAL HEALTH
CLINICAL INFO RESOURCE NETWORK	GENERIC CODE SHEET	MICOM
CLINICAL MONITORING SYSTEM	GRECC	MINIMAL PATIENT DATASET
CLINICAL PROCEDURES	HEALTH DATA & INFORMATICS	MYHEALTHVET
CLINICAL REMINDERS	HEALTH LEVEL SEVEN	Missing Patient Reg (Original) A4EL
CMOP	HEALTH SUMMARY	NATIONAL DRUG FILE
CONSULT/REQUEST TRACKING	HINQ	NATIONAL LABORATORY TEST
CONTROLLED SUBSTANCES	HOSPITAL BASED HOME CARE	NDBI
CPT/HCPCS CODES	ICR - IMMUNOLOGY CASE REGISTRY	NETWORK HEALTH EXCHANGE
CREDENTIALS TRACKING DENTAL DIETETICS	IFCAP IMAGING INCIDENT REPORTING	NOIS NURSING SERVICE OCCURRENCE SCREEN
DISCHARGE SUMMARY	INCOME VERIFICATION MATCH	ONCOLOGY
DRG GROUPER	INCOMPLETE RECORDS TRACKING	ORDER ENTRY/RESULTS REPORTING

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="checkbox"/> 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="checkbox"/> 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="checkbox"/> Who has access to this data?	

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

Title:	Name:	Phone:	Email:
Privacy Officer: Garnett Best	Garnett Best	202-461-7474	Garnett.Best@va.gov
GARNETT S BEST Digitally signed by: GARNETT S BEST DN: CN = GARNETT S BEST O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2010.01.22 15:05:00 -05'00'			
Information Security Officer: Paula Pinckney	Paula Pinckney	301-734-0438	Paula.Pinckney@va.gov
PAULA P PINCKNEY Digitally signed by: PAULA P PINCKNEY DN: CN = PAULA P PINCKNEY O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2010.01.22 11:09:07 -05'00'			
Chief Information Officer:	Joe Gibbons	518-449-0618	Joe.Gibbons@va.gov
Digitally signed by GIBBONS, JOE DN: o=Department of Veterans Affairs, ou=Dept. of Veterans Affairs, Internal Staff, ou=www.verisign.com/repository/CPS Incomp. by Ref.,LIAB.LTD(c)96, cn=GIBBONS, JOE, email=joe.gibbons@va.gov Date: 2010.01.22 11:25:45 -05'00'			
Person Completing Document:	Bernard Brauner	301-734-0369	Bernard.Brauner@va.gov
			
System / Application / Program Manager:		0	0
Digital Signature Block			

Date of Report:

1/22/2010

OMB Unique Project Identifier

029-00-01-11-01-1186-00-105-03-

Project Name

Home Telehealth