

Welcome to the PIA for FY 2011!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vawww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 referenced in the procedure section of this document.

- a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Directive 6508.
- b. Records Officer is responsible for supplying records retention and deletion schedules.
- c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Directive 6508 and to immediately report all anomalies to the Privacy Service and appropriate management chain.
- d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.
- e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

Microsoft Office 2003: To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

Microsoft Office 2007: To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable

All Macros; 2) Click OK

Final Signatures

Final Signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.

Privacy Impact Assessment Uploaded into SMART

Privacy Impact Assessments should be uploaded into C&A section of SMART.

All PIA Validation Letters should be emailed to christina.pettit@va.gov to received full credit for submission.

(FY 2011) PIA: System Identification

Program or System Name: REGION 3 > VHA >

VISN 07 > Dublin VAMC > VistA-VMS

OMB Unique System / Application / Program Identifier 029-00-01-11-01-1180-00

Description of System/ Application/ Program: The VistA 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. The VistA system provides the architecture and foundational elements required to operate and maintain a modern health care IT System. Its subcomponents include: architecture, computing infrastructure, core common services, software, enterprise messaging infrastructure, enterprise terminologies, data standards, and an administrative data repository. All these subcomponents align with the VA's enterprise architecture. The VistA system includes the computer equipment associated with clinical operations and the employees (approximately 800 FTE) necessary to operate the system. VistA is a client-server system. It links the facility computer network to over 100 applications and databases. In 2006, the VistA system supported IT services across the VA organization which had a network of 21 Veterans Integrated Service Networks (VISNs) that managed 155 medical centers, over 881 community based outpatient clinics, 46 residential rehabilitation treatment programs, 135 nursing homes, 207 readjustment counseling centers, 57 veteran benefits regional offices, and 125 national cemeteries. VistA provides critical data that supports the delivery of healthcare to veterans and their dependants. Using the computer, the VA health care provider can access VistA applications and meet a wide range of health care data needs. The VistA system is in the mature phase of the capital investment lifecycle.

Facility Name: DUBLIN VA MEDICAL CENTER

Title:	Name:	Phone:	Email:
Privacy Officer:	FAYE B. MULLIS	478 272-1210X3	faye.mullis@va.gov
Information Security Officer:	JAMES C. AYRES	478 277-2849	james.ayres@va.gov
System Owner/ Chief Information Officer:	JB DIAL	478 277-2700	jb.dial@va.gov
Information Owner:	PATRICK SWINSON	478 277-2716	patrick.swinson@va.gov
Other Titles:			

Person Completing Document: JAMES C. AYRES

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: 10-2009

Date Approval To Operate Expires: 8/29/2011

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.	The VistA-VMS at Carl Vinson VA Medical Center has been operational for 14 years.
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes
If No, please explain:	
Has a PIA been completed within the last three years?	Yes
Date of Report (MM/YYYY):	03/2011

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

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

If there is no Personally Identifiable Information on your system , please complete TAB 7 & TAB 12. (See Comment for Definition of PII)

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.	Yes
For each applicable System(s) of Records, list:	
1. All System of Record Identifier(s) (number):	79VA19
2. Name of the System of Records:	VistA - VMS
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	http://www.va.gov/privacy/Systemsofrecords/
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?	No
Is a Privacy notice provided?	Yes
Proximity and Timing: Is the privacy notice provided at the time of data collection?	Yes
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	Yes
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	Yes
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	Yes

(FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	ALL	The Veterans are told that this information is collected for eligibility purposes and this is conveyed to them via written notice. Also, patients are allowed to download Form 1010 which contains privacy information concerning each of the data fields they are required to enter.	All	All
Family Relation (spouse, children, parents, grandparents, etc)	ALL	The Veterans are told that this information is collected for eligibility purposes and this is conveyed to them via written notice. Also, patients are allowed to download Form 1010 which contains privacy information concerning each of the data fields they are required to enter.	All	All
Service Information	ALL	The Veterans are told that this information is collected for eligibility purposes and this is conveyed to them via written notice. Also, patients are allowed to download Form 1010 which contains privacy information concerning each of the data fields they are required to enter.	All	All

Medical Information	ALL	The Veterans are told that this information is collected for eligibility purposes and this is conveyed to them via written notice. Also, patients are allowed to download Form 1010 which contains privacy information concerning each of the data fields they are required to enter.	All	All
Criminal Record Information	ALL	The Veterans are told that this information is collected for eligibility purposes and this is conveyed to them via written notice. Also, patients are allowed to download Form 1010 which contains privacy information concerning each of the data fields they are required to enter.	All	All
Guardian Information	ALL	The Veterans are told that this information is collected for eligibility purposes and this is conveyed to them via written notice. Also, patients are allowed to download Form 1010 which contains privacy information concerning each of the data fields they are required to enter.	All	All

Medical Information	Yes	Veteran	Mandatory
Criminal Record Information	Yes	Veteran	Mandatory
Guardian Information	Yes	Veteran	Mandatory
Education Information	Yes	Veteran	Mandatory
Benefit Information	Yes	Veteran	Mandatory
Other (Explain)			
Other (Explain)			
Other (Explain)			

(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization		No		N/A	
Other Veteran Organization		No		N/A	
Other Federal Government Agency	Social Security Administration - IRS - DoD	Yes	Name, Social Security Number, date of birth, and sex are transmitted to Social Security Administration. The SSN and first four characters of the surname are transmitted to Internal Revenue Service (IRS) in order to verify certain Veterans' self-reported income with federal tax information to identify Veterans' responsibility for making medical care co-payments and enhance revenue from first party collections. Also, Veteran information is commonly shared with Department of Defense (DoD).	Both PII & PHI	VHA1605.1 and VHA 1605.2 VA HANDBOOKS
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 2011) PIA: Access to Records

Does the system gather information from another system?

No

Please enter the name of the system:

Per responses in Tab 4, does the system gather information from an individual?

Yes

If information is gathered from an

individual, is the information provided:

Through a Written Request

Submitted in Person

Online via Electronic Form

Is there a contingency plan in place to process information when the system is down?

Yes

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?

No

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: N/A

(FY 2011) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

If Yes, Please Specify: NO

Explain how collected data are limited to required elements:

Answer: Data is collected electronically based on the automation of VA forms and clinical procedures. Individuals may either visit the VAMC where they receive their care and begin the process or may visit the Freedom of Information Act (FOIA) website at

<http://www.ga.gov/oit/cio/foia/guide.sap#how> or may go through VA Forms at <http://www.va.gov/vaforms/medical/pdf/vha-10-5345-fill.pdf>.

Further information regard the VA SOR is available at http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SPR_compilation.pdf

How is data checked for completeness?

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

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

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

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

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

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

Answer:

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: Data is maintained in accordance with VA Directive 6300, <http://vaww1.va.gov/vapubs/viewPublication.asp?Pub ID=19&FType=2>, VA Handbook 6300.1, <http://vaww1.va.gov/vapubs/viewPublication.asp?Pub ID=19&FType=2>, and VHA Records Control Schedule 10-1, <http://vaww1.va.gov/vhapublications/rcs10/rcs10-1.pdf>. The final, consolidated, electronic version of a Patient Medical Record, including information migrated from interim electronic information systems, electronic medical equipment, or information entered directly into the patient medical record information system is destroyed/deleted 75 years after the last episode of patient care, in accordance with RCS 10-1, XLIII,2.b., Electronic Final Version of Health Record. Veterans Health Administration (VHA) Records Control Schedule (RCS) 10-1 is the main authority for the retention disposition of VHA records. It provides a brief description of records and states the retention and disposition requirements. It also provides the National Archives and Records Administration (NARA) disposition authorities or the General Records Schedules (GRS) authorities, whichever is appropriate for the records.

In addition to program and services sections, the RCS 10-1 contains a General and Administrative (G&A) Section for records common to several offices and services.

Retention periods for data stored on the LAN vary according to the type of records. Data owners are responsible for ensuring they follow the records retention periods outlined in RCS 10-1.

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

Answer: Veterans Health Administration (VHA) Records Control Schedule (RCS) 10-1 is the main authority for the retention disposition of VHA records. It provides a brief description of records and states the retention and disposition requirements. It also provides the National Archives and Records Administration (NARA) disposition authorities or the General Records Schedules (GRS) authorities, whichever is appropriate for the records. In addition to program and services sections, the RCS 10-1 contains a General and Administrative (G&A) Section for records common to several offices and services. Retention periods for data stored on the LAN vary according to the type of records. Data owners are responsible for ensuring they follow the records retention periods outlined in RCS 10-1.

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

Answer: Electronic Final Version of Patient Medical Records is destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records Control Schedule 10-1, Item XLIII, 2.b. (page 190) At present, VistA Imaging retains all images. We are performing a study to explore whether some images can be eliminated on an earlier schedule.

Where are these procedures documented?

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

How are data retention procedures enforced?

Answer: VA Records Control Schedule 10-1 (page 8) The Health Information Resources Service (HIRS) is responsible for developing policies and procedures for effective and efficient records management throughout VHA. HIRS acts as the liaison between VHA and National Archives and Records Administration (NARA) on issues pertaining to records management practices and procedures. Field records officers are responsible for records management activities at their facilities. Program officials are responsible for creating, maintaining, protecting and disposing of records in their program area in accordance with NARA regulations and VA policy. All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures.

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: YES

(FY 2011) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13? NO

If Yes, How will parental or guardian approval be obtained?

Answer: N/A

(FY 2011) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured. Yes

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls. Yes

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

If 'No' to any of the 3 questions above, please describe why:

Answer:

Is adequate physical security in place to protect against unauthorized access? Yes

If 'No' please describe why:

Answer:

Explain how the project meets IT security requirements and procedures required by federal law.

Answer: At the Department level the CIO's Office of Cyber & Information Security (OCIS) is responsible for the establishment of directives, policies, &

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

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

Answer: (Other Risks) 1. Maintenance and Preventive Maintenance. 2. Application Controls. 3. Construction/Environmental factors. 4. Data integrity/access methodology. 5. Security awareness education and training fo all employees.

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

- Access Control
- Audit and Accountability
- Awareness and Training
- Certification and Accreditation Security Assessments
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Media Protection
- Personnel Security
- Physical and Environmental Protection
- Risk Management

Answer: (Other Controls) 1. Maintenance and preventative maintenance: A majority of LAN/WAN hardware and software maintenance is performed by approved vendors holding repair contracts with OI&T or the facility. OI&T staff perform daily and periodic maintenance to include ensuring hardware components are operational, operating systems are up-to-date, and mandatory software updates, patches, and installations are completed by VA compliance dates. When maintenance is required and downtime is necessary, OI&T staff submit an ANR to notify appropriate parties. This ANR records maintenance actions and readily available for review. Reference VISN 7 Policy 10N7-054, Emergency User Notification of Outages and VISN 7 Policy Memo 10N7-150, IT Maintenance Policy.

2. Application Control: Procedures and policies are in place to grant sufficient and timely access to applications, data, services or other resources needed for authorized individuals to perform their duties. A formal process for requesting access is established and documented through the VISN 7 AIS Operations Security Policy, VISN 7 AIS Access policy, VISN 7 AIS Remote Access Policy, VISN 7 Wireless Restrictions Policy, and Carl Vinson VAMC Memorandum 00-353 Managing Information System User Accounts. Group Policy Objects (GPOs) are also implemented across the various systems which enforce access privileges (to file shares, folders, etc), utilization of removable media (thumb drives, etc.), and session time out parameters. These policies and procedures also document and provide a structure process for terminating access to systems upon termination of individuals from VA employment. Termination process includes a formal clearance process, termination of accounts that have not been accessed in 90 days or more. Periodic reviews of employee access are conducted by Service Line Managers, ADPACs, OI&T Staff and Information Security Officer.

3. Construction/Environmental factors. Physical and environmental factors are adhered to as outlined in VA Directive and Handbook 0730. Windows, doors, locks, alarms, key controls, electronic access, environmental monitoring tools (electricity, fire, water, heat sensors) are provided to meet the requirements of VA Directive and Handbook 0730.

4. Data Integrity/Access Methodology: Several methodologies are in place to ensure data integrity and access to data. First, access must be obtained by an authorized employee with a valid login and password on the Local Area Network. Secondly, the individuals must also obtain a valid and separate VistA access code and password. Access is built around VistA menus which are provided to individuals based upon need to know, least privilege, and approval and authorization from the employee’s supervisor, OI&T department and the Information Security Officer.

5. Security awareness education and training for all employees. This is a mandated requirement and is accomplished through the LMS systems for educations, also, numerous training sessions are conducted though out the year to educate the users. Flyers, pamphlets, and other printed and video material is used to compliment user awareness and education.

PIA: PIA Assessment

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

Answer: Privacy notice.

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?

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.

organization.
(Choose One)

The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?
(Choose One)

The potential impact is **high** if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.

The potential impact is **moderate** if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals.

The potential impact is **low** if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.

Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? (Choose One)

The potential impact is **high** if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.

The potential impact is **moderate** if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals.

The potential impact is **low** if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.

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

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:



(FY 2011) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?
--

Access Manager Actuarial Appraisal System ASSISTS Awards Awards Baker System Bbraun (CP Hemo) BDN Payment History BIRLS C&P Payment System C&P Training Website CONDO PUD Builder Corporate Database Data Warehouse EndoSoft FOCAS Inforce INS - BIRLS Insurance Online Insurance Self Service LGY Home Loans LGY Processing Mobilization Montgomery GI Bill MUSE Omnicell Priv Plus RAI/MDS Right Now Web SAHSHA Script Pro SHARE SHARE SHARE Sidexis Synquest	Automated Sales Reporting (ASR) BCMA Contingency Machines Benefits Delivery Network (BDN) Centralized Property Tracking System Common Security User Manager (CSUM) Compensation and Pension (C&P) Control of Veterans Records (COVERS) Control of Veterans Records (COVERS) Control of Veterans Records (COVERS) Courseware Delivery System (CDS) Dental Records Manager Education Training Website Electronic Appraisal System Electronic Card System (ECS) Electronic Payroll Deduction (EPD) Eligibility Verification Report (EVR) Fiduciary Beneficiary System (FBS) Fiduciary STAR Case Review Financial and Accounting System (FAS) Insurance Unclaimed Liabilities Inventory Management System (IMS) LGY Centralized Fax System Loan Service and Claims Loan Guaranty Training Website Master Veterans Record (MVR) Mental Health Asisstant National Silent Monitoring (NSM) Powerscribe Dictation System Rating Board Automation 2000 (RBA2000) Rating Board Automation 2000 (RBA2000) Rating Board Automation 2000 (RBA2000) Records Locator System Review of Quality (ROQ) Search Participant Profile (SPP) Spinal Bifida Program Ch 18 State Benefits Reference System State of Case/Supplemental (SOC/SSOC)	Automated Folder Processing System (AFPS) Automated Medical Information Exchange II (AIME II) Automated Medical Information System (AMIS)290 Automated Standardized Performace Elements Nationwide (ASPEN) Centralized Accounts Receivable System (CARS) Committee on Waivers and Compromises (COWC) Compensation and Pension (C&P) Record Interchange (CAPRI) Compensation & Pension Training Website Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS) Distribution of Operational Resources (DOOR) Educational Assistance for Members of the Selected Reserve Program CH 1606 Electronic Performance Support System (EPSS) Enterprise Wireless Messaging System (Blackberry) Financial Management Information System (FMI) Hearing Officer Letters and Reports System (HOLAR) Inquiry Routing Information System (IRIS) Modern Awards Process Development (MAP-D) Personnel and Accounting Integrated Data and Fee Basis (PAID) Personal Computer Generated Letters (PCGL) Personnel Information Exchange System (PIES) Personnel Information Exchange System (PIES) Post Vietnam Era educational Program (VEAP) CH 32 Purchase Order Management System (POMS) Reinstatement Entitelment Program for Survivors (REAPS) Reserve Educational Assistance Program CH 1607 Service Member Records Tracking System Survivors and Dependents Education Assistance CH 35 Systematic Technical Accuracy Review (STAR) Training and Performance Support System (TPSS) VA Online Certification of Enrollment (VA-ONCE) VA Reserve Educational Assistance Program Veterans Appeals Control and Locator System (VACOLS) Veterans Assistance Discharge System (VADS) Veterans Exam Request Info System (VERIS) Veterans Service Representative (VSR) Advisor Vocational Rehabilitation & Employment (VR&E) CH 31 Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
---	---	--

VBA Data Warehouse
VBA Training Academy
Veterans Canteen Web
VIC
VR&E Training Website
Web LGY

Telecare Record Manager
VBA Enterprise Messaging System
Veterans On-Line Applications (VONAPP)
Veterans Service Network (VETSNET)
Web Electronic Lender Identification

Web Automated Folder Processing System (WAFPS)
Web Automated Reference Material System (WARMS)
Web Automated Verification of Enrollment
Web-Enabled Approval Management System (WEAMS)
Web Service Medical Records (WebSMR)
Work Study Management System (WSMS)

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system? All are sub-components of our VistA System. ALL

- | | | | |
|---------------|----------------------|-------------------------------|---------------------------------------|
| X ASISTS | X Beneficiary Travel | X Accounts Receivable | X Adverse Reaction Tracking |
| X Bed Control | X Care Management | X ADP Planning (PlanMan) | X Authorization/ Subscription |
| X CAPRI | X Care Tracker | X Bad Code Med Admin | X Auto Replenishment/ Ward Stock |
| X CMOP | X Clinical Reminders | X Clinical Case Registries | X Automated Info Collection Sys |
| X Dental | X CPT/ HCPCS Codes | X Clinical Procedures | X Automated Lab Instruments |
| X Dietetics | X DRG Grouper | X Consult/ Request Tracking | X Automated Med Info Exchange |
| X Fee Basis | X DSS Extracts | X Controlled Substances | X Capacity Management - RUM |
| X GRECC | X Education Tracking | X Credentials Tracking | X Capacity Management Tools |
| X HINQ | X Engineering | X Discharge Summary | X Clinical Info Resource Network |
| X IFCAP | X Event Capture | X Drug Accountability | X Clinical Monitoring System |
| X Imaging | X Extensible Editor | X EEO Complaint Tracking | X Enrollment Application System |
| X Kernal | X Health Summary | X Electronic Signature | X Equipment/ Turn-in Request |
| X Kids | X Incident Reporting | X Event Driven Reporting | X Gen. Med.Rec. - Generator |
| X Lab Service | X Intake/ Output | X External Peer Review | X Health Data and Informatics |
| X Letterman | X Integrated Billing | X Functional Independence | X ICR - Immunology Case Registry |
| X Library | X Lexicon Utility | X Gen. Med. Rec. - I/O | X Income Verification Match |
| X Mailman | X List Manager | X Gen. Med. Rec. - Vitals | X Incomplete Records Tracking |
| X Medicine | X Mental Health | X Generic Code Sheet | X Interim Mangement Support |
| X MICOM | X MyHealthEVet | X Health Level Seven | X Master Patient Index VistA |
| X NDBI | X National Drug File | X Hospital Based Home Care | X Missing Patient Reg (Original) A4EL |
| X NOIS | X Nursing Service | X Inpatient Medications | X Order Entry/ Results Reporting |
| X Oncology | X Occurrence Screen | X Integrated Patient Funds | X PCE Patient Care Encounter |
| X PAID | X Patch Module | X MCCR National Database | X Pharmacy Benefits Mangement |
| X Prosthetics | X Patient Feedback | X Minimal Patient Dataset | X Pharmacy Data Management |
| X QUASER | X Police & Security | X National Laboratory Test | X Pharmacy National Database |
| X RPC Broker | X Problem List | X Network Health Exchange | X Pharmacy Prescription Practice |
| X SAGG | X Progress Notes | X Outpatient Pharmacy | X Quality Assurance Integration |
| X Scheduling | X Record Tracking | X Patient Data Exchange | X Quality Improvement Checklist |
| X Social Work | X Registration | X Patient Representative | X Radiology/ Nuclear Medicine |
| X Surgery | X Run Time Library | X PCE Patient/ HIS Subset | X Release of Information - DSSI |
| X Toolkit | X Survey Generator | X Security Suite Utility Pack | X Remote Order/ Entry System |
| X Unwinder | X Utilization Review | X Shift Change Handoff Tool | X Utility Management Rollup |
| X VA Fileman | X Visit Tracking | X Spinal Cord Dysfunction | X CA Verified Components - DSSI |
| X VBECS | X VistALink Security | X Text Integration Utilities | X Vendor - Document Storage Sys |
| X VDEF | X Women's Health | X VHS & RA Tracking System | X Visual Impairment Service Team ANRV |
| X VistALink | | X Voluntary Timekeeping | X Voluntary Timekeeping National |

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: Minor Applications

Which of these are sub-components of your system?

1184 Web	ENDSOFT	RAFT
A4P	Enterprise Terminology Server & VHA Enterprise Terminology Services	RALS

(FY 2011) PIA: Final Signatures

Facility Name: Dublin VA Medical Center

0

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

Privacy Officer:	FAYE B. MULLIS	478 272-1210X3106	faye.mullis@va.gov
------------------	----------------	-------------------	--------------------

Information Security Officer:	JAMES C. AYRES	478 277-2849	james.ayres@va.gov
-------------------------------	----------------	--------------	--------------------

System Owner/ Chief Information Officer:	JB DIAL	478 277-2700	jb.dial@va.gov
--	---------	--------------	----------------

Information Owner:	PATRICK SWINSON	478 277-2716	patrick.swinson@va.gov
--------------------	-----------------	--------------	------------------------

Other Titles:	0	0	0
---------------	---	---	---

Date of Report: 3/22/11

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

Project Name REGION 3 > VHA .> VISN 07 > DUBLIN VAMC > VistA - VMS

(FY 2011) PIA: Final Signatures

Facility Name: Dublin VA Medical Center

Title: _____ Name: _____ Phone: _____ Email: _____

Privacy Officer: FAYE B. MULLIS 478 272-1210X3106 faye.mullis@va.gov

Information Security Officer: *Faye B Mullis* JAMES C. AYRES 478 277-2849 james.ayres@va.gov

System Owner/ Chief Information Officer: *James C Ayres* JB DIAL 478 277-2700 jb.dial@va.gov

Information Owner: *J.R. Dial* PATRICK SWINSON 478 277-2716 patrick.swinson@va.gov

Other Titles: *Patrick Swinson* 0 0

Date of Report: 3/22/11

OMB Unique Project Identifier: 029-00-01-11-01-1180-00
Project Name: REGION 3 > VHA .> VISN 07 > DUBLIN VAMC > Vista - VMS