

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 > LAN

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

Description of System/ Application/ Program:

The Local Area Network (LAN)/Wide Area Network (WAN) system is a group of servers, computers and associated devices that share a common communications line on which the VHA health care facilities operate their software applications, databases and support for E-Government initiatives. The LAN/WAN has applications and data storage that are shared by multiple users providing portability of information. Without the LAN/WAN, sharing data between applications, databases or other medical centers would not be possible, thus compromising patient care. The LAN/WAN includes the computer equipment associated with clinical operations and the employees (approximately 800 FTE) necessary to operate the system. The LAN/WAN system supports IT services across the VA organization which has 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. The LAN/WAN provides critical data that supports the delivery of healthcare to Veterans, their dependants and employees. Using a computer, the VA health care provider can access all VA applications and meet a wide range of health care and employee data needs. The LAN/WAN system operates in medical centers, community-based clinics, out-reach clinics and Vet Centers. The LAN/WAN 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: | BRAVIS RUNYON | 478 277-2716 | bravis.runyon@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: 8/20/2011

| | |
|---|---|
| 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 LAN/WAN 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.

- | | |
|---|-----|
| <input type="checkbox"/> Have any changes been made to the system since the last PIA? | NO |
| <input checked="" type="checkbox"/> Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA? | YES |
| <input checked="" type="checkbox"/> Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data? | YES |
| <input checked="" type="checkbox"/> Does this system/application/program collect, store or disseminate PII/PHI data? | YES |
| <input checked="" type="checkbox"/> Does this system/application/program collect, store or disseminate the SSN? | YES |

2. System Identification **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.

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?

Is PII collected by paper methods?

Is PII collected by verbal methods?

Is PII collected by automated methods?

Is a Privacy notice provided?

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

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

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

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

Yes

Veterans Health Information Systems and Technology Architecture (VistA) – 79VA19
VistA - VMS

<http://www.va.gov/privacy/Systemsofrecords/>

Yes

No

(Please Select Yes/No)

Yes

Yes

Yes

Yes

Yes

Yes

Yes

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 |
| Education 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 |
| Benefit 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 |
| Other (Explain) | | | | |

| Data Type | Is Data Type Stored on your system? | Source requested. Identify the specific file, entity and/or name of agency) (if requested) | Is data collection Mandatory or Voluntary? | Additional Comments |
|---|-------------------------------------|--|--|---------------------|
| Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc) | Yes | Veteran | Mandatory | |
| Family Relation (spouse, children, parents, grandparents, etc) | Yes | Veteran | Mandatory | |
| Service Information | Yes | Veteran | Mandatory | |
| Medical Information | Yes | Veteran | Mandatory | |
| Criminal Record Information | Yes | 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: | <input type="checkbox"/> Through a Written Request <input checked="" type="checkbox"/> Submitted in Person <input type="checkbox"/> 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: | <input type="checkbox"/> Drug/Alcohol Counseling <input type="checkbox"/> Mental Health <input type="checkbox"/> HIV <input type="checkbox"/> Research <input type="checkbox"/> Sickle Cell <input type="checkbox"/> 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?

No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: Data is collected electronically based on the automation of VA forms and clinical procedures. 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? 75 years

Answer: Clinical information is retained in accordance with VA Records Control Schedule 10-1. Demographic information is updated as applications for care are submitted and retained in accordance with VA Records Control Schedule 10-1.

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

Answer: Clinical information is retained in accordance with VA Records Control Schedule 10-1. Demographic information is updated as applications for care are submitted and retained in accordance with VA Records Control Schedule 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? See Tab 8.

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?

If 'No' please describe why:

Answer: YES

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

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

- | | | |
|--|--|---|
| <input type="checkbox"/> Air Conditioning Failure | <input 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"/> Denial of Service Attacks | <input type="checkbox"/> Power Loss |
| <input type="checkbox"/> Burglary/Break In/Robbery | <input type="checkbox"/> Denial of Service Attacks | <input type="checkbox"/> Sabotage/Terrorism |
| <input type="checkbox"/> Fraud/Asset Misuse | <input type="checkbox"/> Eavesdropping/Interception | <input type="checkbox"/> Storms/Hurricanes |
| <input type="checkbox"/> Communications Loss | <input type="checkbox"/> Errors (Configuration and Data Entry) | <input type="checkbox"/> Substantial Abuse |
| <input type="checkbox"/> Computer Intrusion | <input type="checkbox"/> Fire (False Alarm, Major, and Minor) | <input type="checkbox"/> Theft of Assets |
| <input type="checkbox"/> Computer Misuse | <input type="checkbox"/> Flooding/Water Damage | <input type="checkbox"/> Theft of Data |
| <input type="checkbox"/> Data Destruction | <input type="checkbox"/> Fraud/Embezzlement | <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 for all employees.

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

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

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 OMB or the facility. OMB 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, OMB staff submit an AMR to notify appropriate parties. This AMR records maintenance actions and readily available for review. Reference VSN 7 Policy 120V-054, Emergency User Notification of Outages and VSN 7 Policy Memo 120V-155, 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 VSN 7 AIS Operations Security Policy, VSN 7 AIS Access policy, VSN 7 AIS Remote Access Policy, VSN 7 Wireless Restrictions Policy, and Carl Vinson VAMC Memorandum 00-355 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., installation 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, ADPAC, OMB 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 Visa Access code and password. Access is built around Visa menus which are provided to individuals based upon need to know, least privilege, and approval and authorization from the employee's supervisor, OMB 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 education, also, numerous training sessions are conducted throughout the year to educate the users. Flyers, pamphlets, and other printed and video material is used to complement 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? (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 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 assessment?

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; personnel security; risk assessment; remote and service 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 number and your comments.

How are data retention procedures enforced? NARA, in consultation with commission staff, will review records covered by this item and may identify files that warrant permanent retention. Such records will be transferred to the National Archives on termination of the commission.

stion you are responding to and then add

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?

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

| | | | |
|-------------|--------------------|-----------------------------|-------------------------------------|
| ASISTS | Beneficiary Travel | Accounts Receivable | Adverse Reaction Tracking |
| Bed Control | Care Management | ADP Planning (PlanMan) | Authorization/ Subscription |
| CAPRI | Care Tracker | Bad Code Med Admin | Auto Replenishment/ Ward Stock |
| CMOP | Clinical Reminders | Clinical Case Registries | Automated Info Collection Sys |
| Dental | CPT/ HCPCS Codes | Clinical Procedures | Automated Lab Instruments |
| Dietetics | DRG Grouper | Consult/ Request Tracking | Automated Med Info Exchange |
| Fee Basis | DSS Extracts | Controlled Substances | Capacity Management - RUM |
| GRECC | Education Tracking | Credentials Tracking | Capacity Management Tools |
| HINQ | Engineering | Discharge Summary | Clinical Info Resource Network |
| IFCAP | Event Capture | Drug Accountability | Clinical Monitoring System |
| Imaging | Extensible Editor | EEO Complaint Tracking | Enrollment Application System |
| Kernal | Health Summary | Electronic Signature | Equipment/ Turn-in Request |
| Kids | Incident Reporting | Event Driven Reporting | Gen. Med.Rec. - Generator |
| Lab Service | Intake/ Output | External Peer Review | Health Data and Informatics |
| Letterman | Integrated Billing | Functional Independence | ICR - Immunology Case Registry |
| Library | Lexicon Utility | Gen. Med. Rec. - I/O | Income Verification Match |
| Mailman | List Manager | Gen. Med. Rec. - Vitals | Incomplete Records Tracking |
| Medicine | Mental Health | Generic Code Sheet | Interim Mangement Support |
| MICOM | MyHealthEVet | Health Level Seven | Master Patient Index VistA |
| NDBI | National Drug File | Hospital Based Home Care | Missing Patient Reg (Original) A4EL |
| NOIS | Nursing Service | Inpatient Medications | Order Entry/ Results Reporting |
| Oncology | Occurrence Screen | Integrated Patient Funds | PCE Patient Care Encounter |
| PAID | Patch Module | MCCR National Database | Pharmacy Benefits Mangement |
| Prosthetics | Patient Feedback | Minimal Patient Dataset | Pharmacy Data Management |
| QUASER | Police & Security | National Laboratory Test | Pharmacy National Database |
| RPC Broker | Problem List | Network Health Exchange | Pharmacy Prescription Practice |
| SAGG | Progress Notes | Outpatient Pharmacy | Quality Assurance Integration |
| Scheduling | Record Tracking | Patient Data Exchange | Quality Improvement Checklist |
| Social Work | Registration | Patient Representative | Radiology/ Nuclear Medicine |
| Surgery | Run Time Library | PCE Patient/ HIS Subset | Release of Information - DSSI |
| Toolkit | Survey Generator | Security Suite Utility Pack | Remote Order/ Entry System |
| Unwinder | Utilization Review | Shift Change Handoff Tool | Utility Management Rollup |
| VA Fileman | Visit Tracking | Spinal Cord Dysfunction | CA Verified Components - DSSI |
| VBECS | VistALink Security | Text Integration Utilities | Vendor - Document Storage Sys |
| VDEF | Women's Health | VHS & RA Tracking System | Visual Impairment Service Team ANRV |
| VistALink | | Voluntary Timekeeping | 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 |
| X | Administrative Data Repository (ADR) | ePROMISE | X Remedy Application |
| | ADT | EYECAP | X SAN |
| X | Agent Cashier | Financial and Accounting System (FAS) | X Scanning Exam and Evaluation System |
| X | Air Fortress | X Financial Management System | Sentillion |
| | Auto Instrument | Genesys | Stellant |
| X | Automated Access Request | X Health Summary Contingency | Stentor |
| | BDN 301 | X ICB | Tracking Continuing Education |
| X | Bed Board Management System | KOWA | X Traumatic Brain Injury |
| | Cardiff Teleform | X Lynx Duress Alarm | VA Conference Room Registration |
| | Cardiology Systems (stand alone servers from the network) | X MHTP | VAMedSafe |
| X | CHECKPOINT | X Microsoft Active Directory | VBA Data Warehouse |
| | Clinical Data Repository/Health Data Repository | X Microsoft Exchange E-mail System | |
| | Combat Veteran Outreach Committee on Waiver and Compromises | X Military/Vet Eye Injury Registry | VHAHUNAPP1 |
| | CP&E | Mumps AudioFAX | X VISTA RAD |
| X | Crystal Reports Enterprise | NOAHLINK | Whiteboard |
| X | Data Innovations | Onnicell | |
| | DELIVEREX | Onvicord (VLOG) | |
| | DICTATION-Power Scribe | Optifill | |
| | DRM Plus | X P2000 ROBOT | |
| | DSIT | PACS database | |
| X | DSS Quadramed | Personal Computer Generated Letters | |
| | EDS Whiteboard (AVJED) | X PICIS OR | |
| X | EKG System | PIV Systems | |
| | Embedded Fragment Registry | Q-Matic | |
| | | QMSI Prescription Processing | |

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: Final Signatures

| | | | |
|--|--|-----------------------|----------------------|
| Facility Name: | 0 | | |
| Title: | Name: | Phone: | Email: |
| Privacy Officer: | FAYE B. MULLIS | 478 272-1210 ex, 3106 | faye.mullis@va.gov |
| [Redacted Signature Box] | | | |
| Information Security Officer: | JAMES C. AYRES | 478 277-2849 | james.ayres@va.gov |
| [Redacted Signature Box] | | | |
| System Owner/ Chief Information Officer: | JB DIAL | 478 277-2700 | jb.dial@va.gov |
| [Redacted Signature Box] | | | |
| Information Owner: | BRAVIS RUNYON | 478 277-2716 | bravis.runyon@va.gov |
| [Redacted Signature Box] | | | |
| Other Titles: | 0 | 0 | 0 |
| [Redacted Signature Box] | | | |
| Date of Report: | 3/21/11 | | |
| OMB Unique Project Identifier | 029-00-02-00-01-1120-00 | | |
| Project Name | REGION 3 > VHA > VISN 07 > Dublin VAMC > LAN | | |

(FY 2011) PIA: Final Signatures

Facility Name: Dublin VAMC

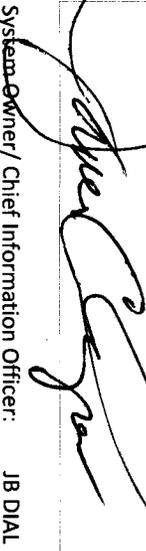
Title: Name:

Privacy Officer: FAVE B. MULLIS

Phone: 478 272-1210 ex, 3106 Email: 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: BRAVIS RUNYON

478 277-2716 bravis.runyon@va.gov


Other Titles:

0 0

Date of Report: 3/21/11
OMB Unique Project Identifier: 029-00-02-00-01-1120-00
Project Name: REGION 3 > VHA > VISN 07 > Dublin VAMC > LAN