

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: Region 3 >VISN 11>Saginaw
VAMC>LAN

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

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

Description of System / Application / Program: education.

Facility Name: Aleda E. Lutz VA Medical Center

| Title: | Name: | Phone: | Email: |
|-------------------------------|----------------------|---------------------|--|
| Privacy Officer: | Deana Bonner | 989-497-2500 x13136 | deana.bonner@va.gov |
| Information Security Officer: | Betty Duchane-Styers | 989-497-2500 x13277 | betty.duchane-styers@va.gov |
| Chief Information Officer: | Stephanie Young | 989-497-2500 x13274 | stephanie.young@va.gov |
| Person Completing Document: | Betty Duchane-Styers | 989-497-2500 x13277 | betty.duchane-styers@va.gov |
| Other Titles:LAN Manager | Pietro Genovese | 989-497-2500 x13284 | pietro.genovese@va.gov |

Other Titles: _____
Other Titles:
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY) 08/2008
Date Approval To Operate Expires: 08/2011

What specific legal authorities authorize this program or system: Title 38, United States Code, section 7301(a).

What is the expected number of individuals that will have their PII stored in this system: Approximately 105,050

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. 18 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):

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?

- Does this system/application/program collect, store or disseminate PII/PHI data?
- Does this system/application/program collect, store or disseminate the SSN?

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

(FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?

Yes

if the answer above is no, please skip to row 16.

For each applicable System(s) of Records, list:

1. All System of Record Identifier(s) (number):

79VA19, 24VA19

2. Name of the System of Records:

VISTA

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

http://www.rms.oit.va.gov/System_of_Records.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?

Yes

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

Yes

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

Yes

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

Yes

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

Yes

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

Yes

(FY 2010) PIA: Notice

Please fill in each column for the data types selected.

| Data Type | Collection Method | What will the subjects be told about the information collection? | How is this message conveyed to them? | How is a privacy notice provided? |
|---|-------------------|--|---------------------------------------|-----------------------------------|
| Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc) | ALL | The most common data types that are captured and accessed on a regular basis by authorized individuals are first and last name, middle initial, DOB, SSN, and address. This patient information falls into two classes: administrative and clinical. Clinical information is used to diagnose, prescribe treatment and follow clinically the patient through his/her health care encounters. Administrative data is used to identify the veteran (SSN), correspond to/from (name and address), and determine eligibility (patient administrative info + SSA and IRS data). | All | All |
| Family Relation (spouse, children, parents, grandparents, etc) | ALL | Dependent Data is utilized to determine eligibility for VA benefits. In addition, NOK and emergency contact information is often a dependent of | All | All |
| Service Information | ALL | service, discharge date, discharge type, service connection rating, medical conditions related to military service, etc). This information is collected to assess eligibility for VA healthcare benefits, type of healthcare needed. | All | All |

VistA-Legacy applications and meet a wide range of health care data needs. The VistA-Legacy system operates in medical centers, ambulatory and community-based clinics, nursing homes and domiciliary, and thus collects a wide range of personal medical information for clinical diagnosis, treatment, patient evaluation, and patient care. Common types of personal medical information would include lab test results, prescriptions, allergies, medical diagnoses, vital signs, etc. The information is used to treat and care for the veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of the veteran.

| | | | | |
|-----------------------------|--------------------------|--|------------------|---------|
| Medical Information | ALL | | All | All |
| Criminal Record Information | Electronic/File Transfer | Criminal record is sent by national law enforcement and stored in locked area in Police Service. Specific information is not input into the VistA system but the fugitive felon program includes a flag on the patient file identifying the need to contact the VA police. | Written | Written |
| Guardian Information | ALL | Guardian information is often flagged in the medical record to ensure the timely and appropriate notification during healthcare decision making from provider/patient/guardian. | All | All |
| Education Information | N/A | | | |
| Benefit Information | Paper & Electronic | VIS, HINQ, VERA, KLF, used to verify service dates, eligibility, SSN, etc. | Verbal & Written | Written |
| Other (Explain) | ALL | In addition insurance and employment information is available on the veteran for use in billing for care. Religious information is collected to provide for spiritual needs if requested by the veteran. | All | All |

| Data Type | Is Data Type Stored on your system? | Source (If requested, identify the specific file, entity and/or name of agency) | Is data collection Mandatory or Voluntary? | Additional Comments |
|---|-------------------------------------|--|--|---------------------|
| Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc) | Yes | Veteran | Mandatory | |
| Family Relation (spouse, children, parents, grandparents, etc) | Yes | Veteran | Mandatory | |
| Service Information | Yes | VA Files / Databases (Identify file) | Mandatory | VBA |
| Medical Information | Yes | Veteran | Mandatory | |
| Criminal Record Information | Yes | Other Federal Agency (Identify) | Mandatory | Fugitive Felon |
| Guardian Information | Yes | State Agency (Identify) | Mandatory | |
| Education Information | Yes | Veteran | Mandatory | |
| Benefit Information | Yes | VA Files / Databases (Identify file) | Mandatory | VBA |
| Other (Explain) | | | | |
| Other (Explain) | | | | |
| Other (Explain) | | | | |

(FY 2010) PIA: Data Sharing

| Organization | Name of Agency/Organization | Do they access this system? | Identify the type of Data Sharing and its purpose. | Is PII or PHI Shared? | What is the procedure you reference for the release of information? |
|-----------------------------------|---|-----------------------------|---|-----------------------|---|
| Internal Sharing: VA Organization | VBA | No | treatment and demographic for benefits determination | Both PII & PHI | MCM-136-10 |
| Other Veteran Organization | Office of Regional Counsel | No | Tort Claims, legal processes | Both PII & PHI | BAA |
| Other Federal Government Agency | Dept of Defense, IRS, Austin Automation, Social Security Administration | No | DoD data used the Health Data Repository to share vital health information, IRS to perform income verification to determine if third party collection is possible. HINQ, VIS is used in determining eligibility for care. AAC is the national processing site for workload at all VA sites. SSA is utilized to validate death and SSNs. | Both PII & PHI | MCM 136-18 |
| State Government Agency | Health Department | No | Mandatory reporting | Both PII & PHI | Standing letter of agreement. |
| Local Government Agency | NO | | | | |
| Research Entity | NO | No | N/A | N/A | |

Other Project / System

In the coordination of care it is often required to gather data from patients receiving co-managed care that entails collecting data from outside sources such as private doctors, labs, xray etc. This is essential in the total care of the patient. This data is collected through release of information methods and is scanned into the system and stored on the FDA approved, secured VistA Imaging Server.

Private sector Providers

No

Both PII & PHI MCM 136-10

Other Project / System

Other Project / System

(FY 2010) PIA: Access to Records

Does the system gather information from another system?

Yes

Please enter the name of the system: DOD, VBA, HINQ, VIS, IRS (IVM), SSA

Name, SSN, DOB, and Sex are transmitted to SSA and the SSN and first four characters of the surname are transmitted to IRS in order to verify certain veteran's self-reported income information with federal tax information to identify veteran's responsibility for making medical care co-payments and enhance revenue from first party collections (Income Verification Match). Also, veteran information is commonly shared with the Department of Defense (DoD). There is certain VHA VistA patient data that is shared with DoD through the Federal/Bidirectional Health Information Exchange (FHIE/BHIE) Program under DUAs that have been in effect for several years. In addition, certain clinical information

No access to 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

check all three

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

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

if yes, please check all that apply:

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: Data is collected electronically based on the automation of VA forms and clinical procedures. DOD sharing agreement would be limited to the required elements by automated mechanisms (this is not paper forms but directly pulled and transmitted from our systems based on pre-designated fields). SSA is based on an automated pull from a pre-built and approved health summary for specific data that can be released to the SSA. (FROM ROI PACKAGE)

How is data checked for completeness?

Answer: Validation of data is reviewed by intake and data analysis staff and compared to paper forms and there are automated VistA system checks for registrations.

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

Answer: Clinical data is reviewed and updated in the patient record at each visit and is electronically signed by the author. Administrative data is updated annually with each application for care and at each patient visit.

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

Answer: New data is compared with printed form ,via patient verification, signed official forms. (birth certificate, SS cards, Picture ID, Driver license, etc.)

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

Answer:

(FY 2010) PIA: Retention & Disposal

What is the data retention period?

Answer: 75 years after the last episode of care.

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.

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

Answer: Electronic Final Version of Patient Medical Record 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).

Where are these procedures documented?

Answer: Record Control Schedule 10-1

How are data retention procedures enforced?

Answer: 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:

(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: The facility follows the Office of Cyber & Information Security (OCIS) established 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 Vista-Legacy is and has been subject to.

Locally, each system is subjected to a security control check list which is implemented prior to a system being placed into service and it is the responsibility of the system manager with oversight by the ISO and CIO. Each checklist is reviewed during the Change Control Board meetings, which is chaired by the CIO no third party software is introduced without being tested and approved by CCB. Any new system must be approved on the IT procurement website which includes documentation and security review before concurrence. All projects which include medical devices go through the local equipment committee which both the ISO and CIO are members. Medical Device security reviews must include the check list that is supplied with VA Directive 6550 before purchase. At the end of the life cycle of the project any data contained on hardware/equipment is mandated to be sanitized via the approved VA method. An IT specialist is required to be a member of any team at the medical center that is initiating a project that may

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

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

Answer: (Other Risks)

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

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

Answer: (Other Controls)

PIA: PIA Assessment

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

Answer: None

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

| | | | | |
|--------------|------|------------------------------|--|----------|
| Minor app #1 | Name | | Description | Comments |
| | | | | |
| | | | Is PII collected by this min or application? | |
| | | | Does this minor application store PII? | |
| | | | If yes, where? | |
| | | Who has access to this data? | | |

| | | | | |
|--------------|------|------------------------------|--|----------|
| Minor app #2 | Name | | Description | Comments |
| | | | | |
| | | | Is PII collected by this min or application? | |
| | | | Does this minor application store PII? | |
| | | | If yes, where? | |
| | | Who has access to this data? | | |

| | | | | |
|--------------|------|------------------------------|--|----------|
| Minor app #3 | 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? | | |

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

| | | | | |
|--------------|------|------------------------------|--|----------|
| 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? | | |

| | |
|---|--|
| 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 |
| | Air Fortress | | Wireless encryption | |
| | | <input type="checkbox"/> NO | Is PII collected by this min or application? | |
| | | <input type="checkbox"/> NO | Does this minor application store PII? | |
| | | | If yes, where? | |
| | | Who has access to this data? | | |

| | | | | |
|--------------|---------|------------------------------|--|------------------|
| Minor app #2 | Name | | Description | Comments |
| | Q-Matic | | Patient Check-In system | Lab and Pharmacy |
| | | <input type="checkbox"/> NO | Is PII collected by this min or application? | |
| | | <input type="checkbox"/> NO | Does this minor application store PII? | |
| | | | If yes, where? | |
| | | Who has access to this data? | | |

| | | | | |
|--------------|------------|---|---|----------|
| Minor app #3 | Name | | Description | Comments |
| | Sentillion | | Synchronizes signon for multiple applications | |
| | | <input type="checkbox"/> NO | Is PII collected by this min or application? | |
| | | <input type="checkbox"/> NO | Does this minor application store PII? | |
| | | | If yes, where? | |
| | | Who has access to this data? OI&T Staff | | |

(FY 2010) PIA: Final Signatures

Facility Name: Aleda E. Lutz VA Medical Center

| Title: | Name: | Phone: | Email: |
|-------------------------------|----------------------|------------------------|-----------------------------|
| Privacy Officer: | Deana Bonner | 989-497-2500 x13136 | deana.bonner@va.gov |
| Digital Signature Block | | | |
| Information Security Officer: | Betty Duchane-Styers | 989-497-2500 x13277 | betty.duchane-styers@va.gov |
| Digital Signature Block | | | |
| Chief Information Officer: | Stephanie Young | 989-497-2500 x13274 | stephanie.young@va.gov |

Digital Signature Block

Person Completing Document: Betty Duchane-Styers

989-497-2500
x13277

betty.duchane-styers@va.gov

System / Application / Program Manager:

System / Application / Program Manager: Pietro Genovese

989-497-2500
x13284

pietro.genovese@va.gov

Digital Signature Block

Date of Report: 1/0/1900
OMB Unique Project Identifier 029-00-02-00-01-1120-00
Project Name Region 3 >VISN 11>Saginaw VAMC>LAN