

(FY 2011) PIA: System Identification

Program or System Name: REGION 5 > VBA > St Paul Region > VARO Chicago > LAN
 OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-02-00-01-1120-00

The Regional Office (RO) Local Area Network (LAN) serves as the default repository for incidental data used and processed by various VBA Major Applications. This data is used in granting compensation, pension, education, vocational rehabilitation and employment, insurance, and loan guaranty benefits to veterans. Information stored also includes data used for various administrative functions. The system provides RO employees local access to file and print sharing services on the LAN. It also provides client access to various applications, including email.

Description of System/ Application/ Program:

Facility Name:

Title:	Name:	Phone:	Email:
Privacy Officer:	Chad D. Peek	(312) 980-4218	Chad.PEEK@va.gov
Information Security Officer:	Jose L. Garcia	(312) 980-4222	Jose.L.Garcia@va.gov
System Owner:	Kevin C. Causley	(202) 461-9170	Kevin.Causley@va.gov
Information Owner:	Duane A. Honeycutt	(312) 980-4203	Duane.Honeycutt1@va.gov
C&A Project Officer:	Mary D. Barley	(202) 461-9175	Mary.Barley@va.gov

Person Completing Document:

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY) 03/2008
 Date Approval To Operate Expires: 08/2011

What specific legal authorities authorize this program or system: Title 38 of the United States Code
 What is the expected number of individuals that will have their PII stored in this system:

1,000,000 – 9,999,999 per last PIA; Although the majority of veteran data is stored in a central database not located at this facility, during the processing of benefits, it is often necessary for employees to store files containing personal information on the network. This is done for a variety of reasons to include but not limited to temporary storage while working a case, for reference purposes, or to assist in case management. These files consist of Excel Spreadsheets and Word Documents stored on shared directories for office access.

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

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.

Operations/Maintenance

The Chicago VARO LAN has been in operation since 04/2004.

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): 02/2011

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 2 & 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):

17VA26, 37VA27, 55VA26, 58VA21/22/28

17VA26 Loan Guaranty Fee Personnel and Program Participant Records-VA. 37VA27 VA Supervised Fiduciary/Beneficiary and General Investigative Records-VA. 55VA26 Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records-VA. 58VA21/22/28 Compensation, Pension, Education, Vocational Rehabilitation and Employment Records-VA, and 103VA07B Police and Security Records-VA.

2. Name of the System of Records:

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

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

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	Benefits	All	All
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Benefits	All	All
Service Information	ALL	Benefits	All	All
Medical Information	ALL	Benefits	All	All
Criminal Record Information	ALL	Benefits	All	All
Guardian Information	ALL	Benefits	All	All
Education Information	ALL	Benefits	All	All
Benefit Information	ALL	Benefits	All	All
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Voluntary	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	
Service Information	Yes	Veteran	Voluntary	
Medical Information	Yes	Veteran	Voluntary	
Criminal Record Information	Yes	Veteran	Voluntary	
Guardian Information	Yes	Veteran	Voluntary	
Education Information	Yes	Veteran	Voluntary	
Benefit Information	Yes	Veteran	Voluntary	
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	Veteran's Health Administration / National Cemetery Administration	Yes	(1) WebHINQ enables VHA to retrieve data from the corporate database and BIRLS. WebHINQ retrieves 4 pieces of data when the record is stored in the corporate database. When available, the following will be retrieved for each SC disability: The affected extremity. The original effective date of the disability rating and the current (most recent) date the rating was changed. In addition, the Effective Date of Combined SC Evaluation is provided. (2) CAPRI enables data flow between VBA and VHA. (3) For the NCA, (IBBA) was used for online retrieval of veteran data. Since Internet BDN/BIRLS Access (IBBA) has been decommissioned, the NCA now utilize SHARE for Beneficiary Identification and Record Location System (BIRLS) Inquiries, Control of Veterans Records (COVERS) Inquiries, National Cemetery Inquiries and First Notice of Death.	Both PII & PHI	VA Directive 6500, M20-4, Part II, VBA IRM Handbook 5.00.02HB2 and M20-4, Part II, VBA IRM Handbook 5.00.02HB4
Other Veteran Organization	Veteran Service Organizations	Yes	Co-located Veterans Service Organizations (VSOs) –Co-located Veterans Service Organizations at VBA regional offices have been given on-line read only access to BDN, BDN Shell, Covers, Share, State Benefits Reference Systems, VACOLS, Virtual VA, Advisory, WARMS and MAP-D. The co-located VSOs have direct access to veteran data securely through LAN. This access is authorized by VA regulations. The organization requests access and the standard VA logon and password security requirements that are applicable to VA employees are followed. Remote Veterans Service Organizations (VSOs) –Remote Veterans Service Organizations have been given on-line read only access to SHARE and MAPD. The remote VSOs access veteran data securely through VA's Virtual Private Network. On-line access is real time and may be accessed by the County/State/National Service Organization at any time. This access is authorized by VA regulations. The County/State/National Service Organization requests on-line access for its representatives. The organization requests access and the standard VA logon and password security	Both PII & PHI	VA Directive 6500, M20-4, Part II, VBA IRM Handbook 5.00.02HB2 and M20-4, Part II, VBA IRM Handbook 5.00.02HB4

Other Federal Government Agency		National Service Life Insurance, Veterans Mortgage Life Insurance, Veterans Government Life Insurance verifies if a veteran is deceased. The Social Security Administration also verifies if a veteran is deceased and provides income verification, SSN match. Department of Defense provides (1) Service Data: reserve and guard participation, retired pay or severance pay, hazardous agent exposure, branch of service, active duty date, released date, type of discharge, separation reason; and (2) Medical Records: Military clinical records, government health records, vocational rehabilitation and employment records, line of duty investigations. Other Federal	Both PII & PHI	VA Directive 6500, M20-4, Part II, VBA IRM Handbook 5.00.02HB2 and M20-4, Part II, VBA IRM Handbook 5.00.02HB4
State Government Agency	Yes	1. To determine eligibility for veteran benefits, either for compensation and pension, education and/or vocational rehabilitation and employment. For example, inquiry to locate and verify status of dependents or to verify a state court decision requiring a veteran to provide care payments in case of separation of marriage.	Both PII & PHI	VA Directive 6500, M20-4, Part II, VBA IRM Handbook 5.00.02HB2 and M20-4, Part II, VBA IRM Handbook 5.00.02HB4
Local Government Agency	No			
Research Entity	No			
Other Project / System	VBA Corporate database and the Benefits Delivery Network database	Data in the VBA Corporate database and the Benefits Delivery Network database are accessed primarily to support the applications running on the LAN.	Both PII & PHI	VA Directive 6500, M20-4, Part II, VBA IRM Handbook 5.00.02HB2 and M20-4, Part II, VBA IRM Handbook 5.00.02HB4
Other Project / System				
Other Project / System				

(FY 2011) PIA: Access to Records

Does the system gather information from another system? Please enter the name of the system:	No
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 checked="" type="checkbox"/> Through a Written Request <input checked="" type="checkbox"/> Submitted in Person <input checked="" 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:	

(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: Information is collected primarily on defined forms and entered to specific fields of database records. The required veteran's data is stored within the databases, which support the individual claim or claims the veteran has been granted. The LAN accesses these databases to retrieve the data.

How is data checked for completeness?

Answer: Per VA Directive 6500, user access is restricted to a need to know basis. The end user access is restricted by the level of authority they require to perform their jobs. The systems include authorization at the application and function level. Users may have inquiry, update (sometimes sub-divided), or verifier authority to different screens.

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

Answer: Most of the major applications that run on the LAN have built in alerts that are flagged if anyone tries to access any veteran data outside of their individual authorization permissions. These alert messages are compiled into daily reports that are provided to the Information Security Officer and are reviewed to verify what incidents took place. Depending on the degree of error, corrective action is followed through. All access can be tracked to individual end-users to identify any unauthorized attempts to access veterans' records. Users also sign a Rules of Behavior prior to system access and annually thereafter.

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

Answer: Most of the major applications that run on the LAN have built in alerts that are flagged if anyone tries to access any veteran data outside of their individual authorization permissions. These alert messages are compiled into daily reports that are provided to the Information Security Officer and are reviewed to verify what incidents took place. Depending on the degree of error, corrective action is followed through. All access can be tracked to individual end-users to identify any unauthorized attempts to access veterans' records. Users also sign a Rules of Behavior prior to system access and annually thereafter.

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: 6 years after the related records are destroyed or after the related records are transferred to the National Archives of the United States,

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

Answer: For Benefits Purposes

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

Answer: In general, support systems retain information until that work in progress is completed and data is committed to master systems and records. The master systems retain data on a permanent basis (beyond the actual death of the veteran). If incidental data is maintained in a user's personal folder on the network, that data is deleted when the employment is terminated.

Where are these procedures documented?

Answer: VA Handbook 6300.5 and Records Control Schedule (RCS) VBA-1, Part 1, Section

How are data retention procedures enforced?

Answer: Management oversight and review enforces data retention policies.

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 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:

(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: An annual assessment of security controls is currently conducted and will continue to be conducted to ensure that IT security requirements are being met. This strategy implements Federal Regulations, VA IT security policy and guidelines, NIST Guidelines and industry best practices. Security is implemented in compliance with VA's guidelines, policies, and mandates.

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) All security risks for each VBA LAN are identified and documented as Plans of Actions & Milestones in the VA's Security Management and Reporting Tool (SMART). This tool can be accessed from the following website - <https://vaww.fisma.va.gov/smart/login.cfm>.

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

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

Answer: (Other Controls) All mitigating controls for each VBA LAN are identified and documented in the SMART tool. This tool can be accessed from the following website - <https://vaww.fisma.va.gov/smart/login.cfm>.

PIA: PIA Assessment

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

Answer: As a result of performing the PIA, continual emphasis and attention will be applied to addressing security and privacy concerns including assuring that collection of data and personal information contains appropriate consent and release information and that all information stored on VBA/Region Five LANs are secured per VA security standards.

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)	<input type="checkbox"/> 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.
	<input checked="" type="checkbox"/> The potential impact is moderate if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
	<input type="checkbox"/> 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)	<input type="checkbox"/> 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.
	<input checked="" type="checkbox"/> The potential impact is moderate if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals.
	<input type="checkbox"/> 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)	<input type="checkbox"/> 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.
	<input checked="" type="checkbox"/> The potential impact is moderate if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals.
	<input type="checkbox"/> 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 VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow NIST SP800-53 moderate impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of this facility's common security controls. These issues are identified and described in the system security plans for the individual information systems.

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

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
Administrative Data Repository (ADR)	ePROMISE	Remedy Application
ADT	EYECAP	SAN
Agent Cashier	Financial and Accounting System (FAS)	Scanning Exam and Evaluation System
Air Fortress	Financial Management System (FMS)	Sentillion
Auto Instrument	Genesys	Stellant
Automated Access Request	Health Summary Contingency	Stentor
BDN 301	ICB	Tracking Continuing Education
Bed Board Management System	KOWA	Traumatic Brain Injury
Cardiff Teleform	Lynx Duress Alarm	VA Conference Room Registration
Cardiology Systems (stand alone servers from the network)	MHTP	VAMedSafe
CHECKPOINT	Microsoft Active Directory	VBA Data Warehouse
Clinical Data Repository/Health Data Repository	Microsoft Exchange E-mail System	VHAHUNAPP1
Combat Veteran Outreach Committee on Waiver and Compromises	Military/Vet Eye Injury Registry	VHAHUNFPC1
CP&E	Mumps AudioFAX	VISTA RAD
Crystal Reports Enterprise	NOAHLINK	Whiteboard
Data Innovations	Omicell	
DELIVEREX	Onvicord (VLOG)	
DICTIONARY-Power Scribe	Optifill	
DRM Plus	P2000 ROBOT	
DSIT	PACS database	
DSS Quadramed	Personal Computer Generated Letters	
EDS Whiteboard (AVJED)	PICIS OR	
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. 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?

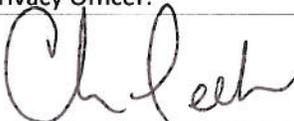
Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: Final Signatures

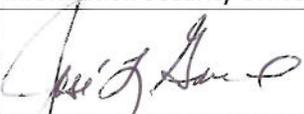
Facility Name: REGION 5 > VBA > St Paul Region > VARO Chicago > LAN

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

Privacy Officer:	Chad D. Peek	(312) 980-4218	Chad.PEEK@va.gov
------------------	--------------	----------------	------------------

 *6-16-2011*
 Digital Signature Block

Information Security Officer:	Jose L. Garcia	(312) 980-4222	Jose.L.Garcia@va.gov
-------------------------------	----------------	----------------	----------------------

 *6/16/2011*
 Digital Signature Block

System Owner:	Kevin C. Causley	(202) 461-9170	Kevin.Causley@va.gov
---------------	------------------	----------------	----------------------

 *6-16-11*
 Digitally signed by Kevin Causley
 DN: cn=US, o=U.S. Government, ou=Department of Veterans Affairs, ou=Internal Staff, 0.9.2342.192.00300.100.1.1=kevin.causley@va.gov, cn=Kevin Causley
 Date: 2011.06.16 07:13:17 -0400
 Digital Signature Block

Information Owner:	Duane A. Honeycutt	(312) 980-4203	Duane.Honeycutt1@va.gov
--------------------	--------------------	----------------	-------------------------


 Digital Signature Block

C&A Project Officer:	Mary D. Barley	(202) 461-9175	Mary.Barley@va.gov
----------------------	----------------	----------------	--------------------

 *6-16-11*
 Digitally signed by Mary Barley
 DN: cn=US, o=U.S. Government, ou=Department of Veterans Affairs, ou=Internal Staff, 0.9.2342.192.00300.100.1.1=mary.barley@va.gov, cn=Mary Barley
 Date: 2011.06.16 07:13:48 -0400
 Digital Signature Block

Date of Report: 5/9/11
 OMB Unique Project Identifier: 029-00-02-00-01-1120-00
 Project Name: REGION 5 > VBA > St Paul Region > VARO Chicago > LAN