

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: Region2>VHA>VISN12>Chicago VAMC>LAN
 OMB Unique System / Application / Program Identifier (AKA: UPID #):

The LAN system is comprised of network devices that support communications, to include routers, switches, disk drives, and uninterruptible power supplies in all wide regions called, "Veterans Integrated Services." A description of their system within this plan.

Access to the system is via workstations operating on Windows XP, thin client terminals, and various models of Windows client workstations connect over a network using Remote Procedure Call (RPC) Broker to connect to both the VA's wide area network (WAN) and the LAN. They are positioned between the Intranet and the Internet.

Description of System/ Application/ Program:

Facility Name:	Jesse Brown VAMC	
Title:	Name:	Phone:
Privacy Officer:	Kristen Ellis	312-569-6117
Information Security Officer:	Jessica Van Benthuysen	312-569-6652
System Owner/ Delegation of Authority	Jeff Fears for BK Hack	708-492-3987
Other Titles: Facility Chief Information Officer	Howard Loewenstein	312-569-6511
Other Titles: Information Security Officer	Maurice Loggins	312-569-6779
Person Completing Document: Information Security Officer	Maurice Loggins	312-569-6779
Other Titles:Deputy Facility Chief Information Officer	Felton Smith	312-569-6483
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)		
Date Approval To Operate Expires:		

What specific legal authorities authorize this program or system:

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

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

2. System Identification

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.

Is there an authorized change control process which documents any changes to existing applications or systems?

If No, please explain:

Has a PIA been completed within the last three years?

Date of Report (MM/YYYY):

Please check the appropriate boxes and continue to the next TAB and complete the remaining

- 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 & TA

029-00-02-00-01-1120-00

ices, workstations, terminals, servers, printers, and other devices which hubs, switches, firewalls, etc. The LAN includes magnetic tape drives, es (UPS), all of which are used at various locations in over 20 nation-vice Networks (VISNs).” Each facility will document their own physical

ating on Windows-family Operating Systems (O/S) including Windows of “dumb” terminals located throughout a Medical Center. Microsoft Windows network and may use terminal emulation software and the xct to other systems, such as Vista. There is access from the Intranet to to the Internet via the VA Internet Gateways. VA-approved firewalls Internet Gateways

Email:

Kristen.Ellis@va.gov

Jessica.VanBenthuyzen@va.gov

jeff.fears@va.gov

Howard.Loewenstein@va.gov

Maurice.Loggins@va.gov

Maurice.Loggins@va.gov

Felton.Smith@va.gov

07/2009

08/2011

Title 38, United States Code, Section 501(b) and Section 304.

293836

Operations/Maintenance
2. System Identification

25 years

Yes

Yes

05/2011

g questions on this form.

employees, contractors, or others performing work for the VA?

of name, unique identifier, symbol, or other PII data?

B 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):

24VA19

2. Name of the System of Records:

Patient Medical 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/24VA19.asp

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?

Yes

Does the System of Records Notice require modification or updating?

No

(Please Select Yes/No)

Is PII collected by paper methods?

Yes

Is PII collected by verbal methods?

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 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)	Verbal	Benefits	Verbally	All
Family Relation (spouse, children, parents, grandparents, etc)	Verbal	Benefits	Verbally	All
Service Information	Verbal	Benefits	Verbally	All
Medical Information	N/A			
Criminal Record Information	ALL	Benefits	Verbally	All
Guardian Information	Verbal	Benefits	Verbally	All
Education Information	Verbal	Benefits	Verbally	All
Benefit Information	Verbal	Benefits	Verbally	All
Other (Explain)	Verbal	Benefits	Verbally	All
Next of Kin	Verbal	Benefits	Verbally	Paper
Death Outside VA	Paper	Benefits	Verbally	Paper
Employment Information	Verbal	Benefits	Verbally	Paper

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	Veteran	Mandatory	

Medical Information	Yes	Veteran	Mandatory
Criminal Record Information	No		
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		No		N/A	
State Government Agency		No		N/A	
Local Government Agency		No		N/A	
Research Entity	Northwestern University	Yes	Research and Development	Both PII & PHI	1605.1 Privacy and Release of information
Other Project / System	University of Illinois of Chicago	Yes	Research and Development	Both PII & PHI	1605.1 Privacy and Release of information
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?		Yes
Please enter the name of the system:	Chicago VAMC . VistA 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 checked="" type="checkbox"/> Through a Written Request <input 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?		Yes
if yes, please check all that apply:	<input checked="" type="checkbox"/> Drug/Alcohol Counseling <input checked="" type="checkbox"/> Research <input checked="" type="checkbox"/> Mental Health <input checked="" type="checkbox"/> Sickle Cell <input checked="" type="checkbox"/> HIV <input type="checkbox"/> Other (Please Explain)	

Describe process for authorizing access to this data.

Answer: Routine Use: HIPAA Authorization; HIPAA Waiver

(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. User access is limited therefore their ability to collect data is also limited. Access is limited by menu and key assignments. Access is based on job function. Access to service directories on LAN is requested and approved by supervisors.

How is data checked for completeness?

Answer: Supervisor reviews information prior to release.

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

Answer: Each service has their own internal policies and procedures for checking data input for completeness. Data is reviewed by supervisors and staff and compared to paper forms where available.

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

Answer: New data is compared with printed form if available, or by comparison to previously entered data.

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: 75 years after the patient dies

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

Answer: Medical Records per Policy

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

Answer: Follow RCS 10-1 as well as facility procedure for PII destruction.

Where are these procedures documented?

Answer: Rcs 10-1

How are data retention procedures enforced?

Answer: No records are disposed/destroyed without approval of the Record Control Manager. All records are disposed of in accordance with VA Policy and disposition authority.

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: We ensure system is compliant with FISMA 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 checked="" type="checkbox"/> Hardware Failure |
| <input checked="" type="checkbox"/> Chemical/Biological Contamination | <input type="checkbox"/> Data Integrity Loss | <input type="checkbox"/> Identity Theft |
| <input checked="" type="checkbox"/> Blackmail | <input checked="" type="checkbox"/> Denial of Service Attacks | <input checked="" type="checkbox"/> Malicious Code |
| <input checked="" type="checkbox"/> Bomb Threats | <input type="checkbox"/> Earthquakes | <input type="checkbox"/> Power Loss |
| <input checked="" type="checkbox"/> Burglary/Break In/Robbery | <input type="checkbox"/> Eavesdropping/Interception | <input type="checkbox"/> Sabotage/Terrorism |
| <input checked="" type="checkbox"/> Cold/Frost/Snow | <input checked="" type="checkbox"/> Errors (Configuration and Data Entry) | <input checked="" type="checkbox"/> Storms/Hurricanes |
| <input checked="" type="checkbox"/> Communications Loss | <input type="checkbox"/> Fire (False Alarm, Major, and Minor) | <input type="checkbox"/> Substance Abuse |
| <input checked="" type="checkbox"/> Computer Intrusion | <input checked="" type="checkbox"/> Flooding/Water Damage | <input checked="" type="checkbox"/> Theft of Assets |
| <input checked="" 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)

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)

PIA: PIA Assessment

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

Answer: Review of privacy notice, data protection methods and review security controls.

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

Please add additional controls:

(FY 2011) PIA: Additional Comments

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

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?

Access Manager	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
x ASSISTS	Centralized Property Tracking System	Automated Standardized Performace 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 Entitelment Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
x MUSE	Mental Health Asisstant	Service Member Records Tracking System
x Omnicell	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
x 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
VBA Training Academy
Veterans Canteen Web
VIC
VR&E Training Website
Web LGY

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

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

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

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

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

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

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

X ASISTS	Beneficiary Travel	X Accounts Receivable	X Adverse Reaction Tracking
X Bed Control	Care Management	ADP Planning (PlanMan)	Authorization/ Subscription
X CAPRI	Care Tracker	Bad Code Med Admin	Auto Replenishment/ Ward Stock
CMOP	Clinical Reminders	Clinical Case Registries	Automated Info Collection Sys
X Dental	CPT/ HCPCS Codes	Clinical Procedures	X Automated Lab Instruments
Dietetics	DRG Grouper	Consult/ Request Tracking	Automated Med Info Exchange
X Fee Basis	DSS Extracts	Controlled Substances	Capacity Management - RUM
GRECC	X Education Tracking	X Credentials Tracking	Capacity Management Tools
HINQ	Engineering	X Discharge Summary	Clinical Info Resource Network
X IFCAP	Event Capture	Drug Accountability	Clinical Monitoring System
X Imaging	Extensible Editor	X EEO Complaint Tracking	Enrollment Application System
Kernal	Health Summary	Electronic Signature	X 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
X Library	Lexicon Utility	Gen. Med. Rec. - I/O	Income Verification Match
X Mailman	List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine	Mental Health	Generic Code Sheet	Interim Mangement Support
MICOM	X MyHealthEVet	Health Level Seven	Master Patient Index VistA
NDBI	National Drug File	X Hospital Based Home Care	X Missing Patient Reg (Original) A4EL
NOIS	Nursing Service	Inpatient Medications	Order Entry/ Results Reporting
Oncology	Occurrence Screen	Integrated Patient Funds	PCE Patient Care Encounter
X PAID	Patch Module	X MCCR National Database	Pharmacy Benefits Mangement
X Prosthetics	Patient Feedback	Minimal Patient Dataset	Pharmacy Data Management
QUASER	X Police & Security	National Laboratory Test	Pharmacy National Database
RPC Broker	Problem List	Network Health Exchange	Pharmacy Prescription Practice
SAGG	X Progress Notes	X Outpatient Pharmacy	Quality Assurance Integration
X Scheduling	Record Tracking	Patient Data Exchange	Quality Improvement Checklist
X Social Work	X Registration	Patient Representative	Radiology/ Nuclear Medicine
X Surgery	Run Time Library	PCE Patient/ HIS Subset	X 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	X 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

(FY 2011) PIA: Final Signatures

Facility Name: Region2>VHA>VISN12>Chicago VAMC>LAN

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

Privacy Officer:	Kristen Ellis	312-569-6117
------------------	---------------	--------------

Digital Signature Block		
-------------------------	--	--

Information Security Officer:	Jessica Van Benthuisen	312-569-6652
-------------------------------	------------------------	--------------

Digital Signature Block		
-------------------------	--	--

System Owner/ Delegation of Authority	Jeff Fears for BK Hack	708-492-3987
---------------------------------------	------------------------	--------------

Digital Signature Block		
-------------------------	--	--

Other Titles: Facility Chief Information Officer	Howard Loewenstein	312-569-6511
--------------------------------------------------	--------------------	--------------

Digital Signature Block		
-------------------------	--	--

Other Titles: Information Security Officer	Maurice Loggins	312-569-6779
--------------------------------------------	-----------------	--------------

Digital Signature Block		
-------------------------	--	--

Date of Report: 5/1/11

OMB Unique Project Identifier 029-00-02-00-01-1120-00

Project Name Region2>Vha>VISN12>Chicago VAMC>LAN

Email:

Kristen.Ellis@va.gov

Jessica.VanBenthuisen@va.gov

jeff.fears@va.gov

Howard.Loewenstein@va.gov

Maurice.Loggins@va.gov