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://vaww.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 indentify 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 submissi

(FY 2011) PIA: System Identification

Program or System Name:	Region 1>VHA>VISN18>Northern Arizona HCS (Prescott)>LAN
OMB Unique System / Application / Program Identifier (AKA: UPID #):	029-00-02-00-01-1120-00
Description of System/ Application/ Program:	VA Health Care System (Prescott VAMC) uses the 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 the delivery of medication, supply management, decision support, medical research, and education

Facility Name: Northern Arizona HCS

Title:	Name:	Phone:	Email:
Privacy Officer:	Lori K Rosenberg	928-445-4860 ext 6088	lori.rosenberg@va.gov
Information Security Officer:	Mike Caldwell	928-776-6096	mike.caldwell@va.gov
System Owner/ Chief Information Officer:	Scott McCrimmon	928-776-6186	scott.mcrimmon@va.gov
Information Owner:	Donna K. Jacobs	928-445-4860 ext 6553	donna.jacobs@va.gov
Other Titles: LAN Manager	Ron Green	928-776-6106	ronald.green@va.gov
Person Completing Document:	Ron Green	928-776-6106	ronald.green@va.gov
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:	100,000
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.	11 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):	01/2011

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

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

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

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.	Yes
For each applicable System(s) of Records, list:	
1. All System of Record Identifier(s) (number):	24VA19
2. Name of the System of Records:	Patient Medical Records-VA
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	http://edocket.access.gpo.gov/2009/pdf/E9-27786.pdf
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	Healthcare	Verbally	Verbally
Family Relation (spouse, children, parents, grandparents, etc)	VA File Database	Healthcare	Verbally	Written
Service Information	Electronic/File Transfer	Healthcare	Verbal & Written	Verbal & Written
Medical Information	VA File Database	Healthcare	Verbal & Written	Verbal & Written
Criminal Record Information	Electronic/File Transfer	Healthcare	Verbal & Written	Verbal & Written
Guardian Information	Verbal			
Education Information	Verbal			
Benefit Information	Verbal			
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	Mandatory	
Medical Information	Yes	Veteran	Voluntary	

Criminal Record Information	No	Other Federal Agency (Identify)		OPM
Guardian Information	Yes	Veteran	Voluntary	
Education Information	No	Veteran	Voluntary	
Benefit Information	Yes	Local Agency (Identify)	Mandatory	HINQ
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	Other VAMC, VBA	Yes	Clinical and Admin	Both PII & PHI	HCSM 136-PB-07 Release of Information
Other Veteran Organization	No	No			
Other Federal Government Agency	CDC	No	Clinical - Statistical	Both PII & PHI	HCSM 136-PB-07 Release of Information
State Government Agency					
Local Government Agency		No			
Research Entity		No			
Other Project / System	Alpha Transcription (Remote Users)	Yes	Clinical data transcription	Both PII & PHI	Business Associate Agreements or MOU
Other Project / System	Allied/IQOR (Remote Users)	Yes	Insurance Verification	Both PII & PHI	Business Associate Agreements or MOU
Other Project / System	S&S Datalink (Remote User)	Yes	Billing claims verification	Both PII & PHI	Business Associate Agreement or MOU
Other Project / System	WVMI (Remote Users)	Yes	EPRP Review	Both PII & PHI	Business Associate Agreement and Contract
Other Project / System	Templeton (Remote Users)	Yes	Imaging Reads	Both PII & PHI	Business Associate Agreement or MOU

(FY 2011) PIA: Access to Records

Does the system gather information from another system?	Yes
Please enter the name of the system:	Region 1 VHA VISN 18 Prescott VAMC VistA
Per responses in Tab 4, does the system gather information from an individual?	No
If information is gathered from an individual, is the information provided:	☐ Through a Written Request ☐ Submitted in Person ☐ Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	Yes

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?	No

5. Data Sharing & Access

if yes, please check all that apply: ☐ [illegible] ☐ Mental Health ☐ HIV ☐ Research ☐ Sickle Cell ☐ Other (Please Explain)

☐ Research ☐ 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: Process is governed by the use of templates, owned by the application

How is data checked for completeness?

Answer: Pulls data from VistA - accuracy is responsibility of application owner

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

Answer: Pulls current data from VistA

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

Answer: Responsibility of the application owner

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 yrs after the last episode of patient care.

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

Answer: for healthcare

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). At the present time, VistA Imaging retains all imagages

Where are these procedures documented?

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

How are data retention procedures enforced?

Answer: Monthly Monitors & Risk Assessments

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: The Northern Arizona Healthcare System follows VA directives, policies, and procedures, to ensuring the security controls for the system are in place and meet the requirements for protecting VA networks.

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

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

Answer: (Other Risks)

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

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

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: Consideration of performing Risk Assessments and Privacy Impact Assessments on individual components of the LAN

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)**

- [x]
- [ ]
- [ ]

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)**

- [x]
- [ ]
- [ ]

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)**

- [x]
- [ ]
- [ ]

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.

As a general support system, the LAN may store and deliver PII to and from the desktop systems and servers as part of it's function. The LAN itself exercises no control over the content of data being stored or transmitted. Review of content is the responsibility of the end user of the LAN and/or the application that is being utilized via the LAN.

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?

Access Manager
Actuarial
Appraisal System
ASSISTS
Awards
Awards
Baker System
Bbraun (CP Hemo)
BDN Payment History
BIRLS
C&P Payment System
C&P Training Website
CONDO PUD Builder
Corporate Database
Data Warehouse
EndoSoft
FOCAS
Inforce
INS - BIRLS
Insurance Online
Insurance Self Service
LGY Home Loans
LGY Processing
Mobilization
Montgomery GI Bill
MUSE
Omnicell
Priv Plus
RAI/MDS
Right Now Web
SAHSHA
Script Pro
SHARE
SHARE
SHARE
Sidexis
Synquest

Automated Sales Reporting (ASR)
BCMA Contingency Machines
Benefits Delivery Network (BDN)
Centralized Property Tracking System
Common Security User Manager (CSUM)
Compensation and Pension (C&P)
Control of Veterans Records (COVERS)
Control of Veterans Records (COVERS)
Control of Veterans Records (COVERS)
Courseware Delivery System (CDS)
Dental Records Manager
Education Training Website
Electronic Appraisal System
Electronic Card System (ECS)
Electronic Payroll Deduction (EPD)
Eligibility Verification Report (EVR)
Fiduciary Beneficiary System (FBS)
Fiduciary STAR Case Review
Financial and Accounting System (FAS)
Insurance Unclaimed Liabilities
Inventory Management System (IMS)
LGY Centralized Fax System
Loan Service and Claims
Loan Guaranty Training Website
Master Veterans Record (MVR)
Mental Health Asisstant
National Silent Monitoring (NSM)
Powerscribe Dictation System
Rating Board Automation 2000 (RBA2000)
Rating Board Automation 2000 (RBA2000)
Rating Board Automation 2000 (RBA2000)
Records Locator System
Review of Quality (ROQ)
Search Participant Profile (SPP)
Spinal Bifida Program Ch 18
State Benefits Reference System
State of Case/Supplemental (SOC/SSOC)

Automated Folder Processing System (AFPS)
Automated Medical Information Exchange II (AIME II)
Automated Medical Information System (AMIS)290
Automated Standardized Performace Elements Nationwide (ASPEN)
Centralized Accounts Receivable System (CARS)
Committee on Waivers and Compromises (COWC)
Compensation and Pension (C&P) Record Interchange (CAPRI)
Compensation & Pension Training Website
Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
Distribution of Operational Resources (DOOR)
Educational Assistance for Members of the Selected Reserve Program CH 1606
Electronic Performance Support System (EPSS)
Enterprise Wireless Messaging System (Blackberry)
Financial Management Information System (FMI)
Hearing Officer Letters and Reports System (HOLAR)
Inquiry Routing Information System (IRIS)
Modern Awards Process Development (MAP-D)
Personnel and Accounting Integrated Data and Fee Basis (PAID)
Personal Computer Generated Letters (PCGL)
Personnel Information Exchange System (PIES)
Personnel Information Exchange System (PIES)
Post Vietnam Era educational Program (VEAP) CH 32
Purchase Order Management System (POMS)
Reinstatement Entitelment Program for Survivors (REAPS)
Reserve Educational Assistance Program CH 1607
Service Member Records Tracking System
Survivors and Dependents Education Assistance CH 35
Systematic Technical Accuracy Review (STAR)
Training and Performance Support System (TPSS)
VA Online Certification of Enrollment (VA-ONCE
VA Reserve Educational Assistance Program
Veterans Appeals Control and Locator System (VACOLS)
Veterans Assistance Discharge System (VADS)
Veterans Exam Request Info System (VERIS)
Veterans Service Representative (VSR) Advisor
Vocational Rehabilitation & Employment (VR&E) CH 31
Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

VBA Data Warehouse
VBA Training Academy
Veterans Canteen Web
VIC
VR&E Training Website
Web LGY
Telecare Record Manager
VBA Enterprise Messaging System
Veterans On-Line Applications (VONAPP)
Veterans Service Network (VETSNET)
Web Electronic Lender Identification
Web Automated Folder Processing System (WAFPS)
Web Automated Reference Material System (WARMS)
Web Automated Verification of Enrollment
Web-Enabled Approval Management System (WEAMS)
Web Service Medical Records (WebSMR)
Work Study Management System (WSMS)

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

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

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

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

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

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 Vertified 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
	A4P
	Administrative Data Repository (ADR)
	ADT
	Agent Cashier
✓	Air Fortress
✓	Auto Instrument
	Automated Access Request
	BDN 301
	Bed Board Management System
	Cardiff Teleform
✓	Cardiology Systems (stand alone servers from the network)
	CHECKPOINT
	Clinical Data Repository/Health Data Repository
	Combat Veteran Outreach
	Committee on Waiver and Compromises
	CP&E
	Crystal Reports Enterprise
✓	Data Innovations
	DELIVEREX
✓	DICTATION-Power Scribe
✓	DRM Plus
	DSIT
✓	DSS Quadramed
	EDS Whiteboard (AVJED)
	ENDSOFT
✓	Enterprise Terminology Server & VHA Enterprise Terminology Services
✓	ePROMISE
	EYECAP
	Financial and Accounting System (FAS)
✓	Financial Management System
	Genesys
	Health Summary Contingency
✓	ICB
	KOWA
	Lynx Duress Alarm
	MHTP
✓	Microsoft Active Directory
✓	Microsoft Exchange E-mail System
	Military/Vet Eye Injury Registry
✓	Mumps AudioFAX
	NOAHLINK
	Omnicell
	Onvicord (VLOG)
	Optifill
	P2000 ROBOT
	PACS database
	Personal Computer Generated Letters
	PICIS OR
✓	PIV Systems
	RAFT
	RALS
	Remedy Application
	SAN
	Scanning Exam and Evaluation System
✓	Sentillion
	Stellant
	Stentor
	Tracking Continuing Education
	Traumatic Brain Injury
	VA Conference Room Registration
	VAMedSafe
	VBA Data Warehouse
	VHAHUNAPP1
	VHAHUNFPC1
	VISTA RAD
	Whiteboard

✓ EKG System	Q-Matic
Embedded Fragment Registry	QMSI Prescription Processing

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

Name	Credit Card Authentication	
Description	Canteen Credit Card Authentication devices on their own VLAN/Subnet	
Comments	VCS Control - on their own VLAN and Subnet	
Is PII collected by this minor application?		YES
Does this minor application store PII?		YES
If yes, where?	VCS	
Who has access to this data?	VCS	

Name	ShoreTel	
Description	Voice Over IP telephone system	
Comments	On it's own VLAN and subnet	
Is PII collected by this minor application?		NO
Does this minor application store PII?	No	NO
If yes, where?	N/A	
Who has access to this data?	N/A	

Name	Pyxis	
Description	Pharmacy and Supply distribution	
Comments	Behind the firewall, on their own VLAN and subnet	
Is PII collected by this minor application?		YES
Does this minor application store PII?		YES
If yes, where?	On the Pyxis Modalities	
Who has access to this data?	Pharmacy and Supply Staff - vendor during VPN access or maintenance	

Name	National Cemetary Association	
Description	PC managed locally, data and user accounts are NCA	
Comments	PC managed locally, data and user accounts are NCA	
Is PII collected by this minor application?	Likely as part of NCA	YES
Does this minor application store PII?		YES
If yes, where?	NCA database	
Who has access to this data?	NCA personnel	

Name	CareTracker
Description	Resource Systems - Activities of Daily Living database for Nursing Home
Comments	Resource Systems - Activities of Daily Living database for Nursing Home
Is PII collected by this minor application?	YES
Does this minor application store PII?	YES
If yes, where?	CareTracker Server
Who has access to this data?	Only local VA staff - primary Nursing Home

Name	AutoMed
Description	ATI (outpatient pharm dispensing) and EXP (inpatient pharm dispensing)
Comments	Behind the firewall, on it's own VLAN and subnet
Is PII collected by this minor application?	YES
Does this minor application store PII?	YES
If yes, where?	AutoMed Server in the Pharmacy
Who has access to this data?	Pharmacy personnel

Name	TopCon
Description	TeleRetinopathy
Comments	Two Local and one remote - interfaced to VistA Imaging (store and forward)
Is PII collected by this minor application?	YES
Does this minor application store PII?	YES
If yes, where?	Temporarily on TopCon workstation - until sent to Vista Imaging
Who has access to this data?	Eye Clinic and VistA Imaging

Name	Temp Trak
Description	Cooper-Atkins Vendor
Comments	Monitors clinical and nutrition freezer and
Is PII collected by this minor application?	NO
Does this minor application store PII?	NO
If yes, where?	
Who has access to this data?	

Name	VBECS
Description	VistA Blood Establishment Computer Software
Comments	Lab Package
Is PII collected by this minor application?	YES
Does this minor application store PII?	YES
If yes, where?	VistA and VBECS server at Region 1
Who has access to this data?	Lab Personnel and VBECS support staff

Name	Non Commercial PACS (VistA Imaging)
Description	Imaging Modalities - picture archiving - VA developed
Comments	
Is PII collected by this minor application?	YES
Does this minor application store PII?	YES
If yes, where?	VistA Imaging Servers, VistA and VistA Imaging Jukebox
Who has access to this data?	Clinicians, HP with VA Staff Accompaniment, Kodak for Jukebox Maint.

Name	VIX
Description	VistA Imaging Exchange - VA Developed
Comments	Sharing patient images between VA's and Department of Defense
Is PII collected by this minor application?	YES
Does this minor application store PII?	YES
If yes, where?	VistA Imaging Servers, VistA and VistA Imaging Jukebox
Who has access to this data?	Clinicians, HP with VA Staff Accompaniment, Kodak for Jukebox Maint.

Name	Accu-Med (Accu-Care)
Description	Nursing Home Software - client-server
Comments	Documentation of care - reporting tool
Is PII collected by this minor application?	YES
Does this minor application store PII?	YES
If yes, where?	Accu-Med Server Database and backup
Who has access to this data?	Nursing Home Staff, server support

Name	Vitria BusinessWare
Description	Interface engine
Comments	Interface communication between data systems
Is PII collected by this minor application?	YES
Does this minor application store PII?	NO
If yes, where?	Vitra BusinessWare Support
Who has access to this data?	Vitria Support, VistA users, application/dB servers

(FY 2011) PIA: Final Signatures

Facility Name: Region 1>VHA>VISN18>Northern Arizona HCS (Prescott)>LAN

Title:	Name:	Phone:	Email:
Privacy Officer:	Lori K Rosenberg	928-445-4860 ext 6088	lori.rosenberg@va.gov
Digital Signature Block			
Information Security Officer:	Mike Caldwell	928-776-6096	mike.caldwell@va.gov
Digital Signature Block			
System Owner/ Chief Information Officer:	Scott McCrimmon	928-776-6186	scott.mcrimmon@va.gov
Digital Signature Block			
Information Owner:	Donna K. Jacobs	928-445-4860 ext 6553	donna.jacobs@va.gov
Digital Signature Block			
Other Titles: LAN Manager	Ron Green	928-776-6106	ronald.green@va.gov
Digital Signature Block			

Date of Report: January 10, 2011 1/0/00

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

Project Name Region 1>VHA>VISN18>Northern Arizona HCS (Prescott)>LAN