(FY 2011) PIA: System Identification

Program or System Name:	REGION 1>VHA>VISN 20>Alaska HCS (Anchorage)>Vista-VMS	
OMB Unique System / Application / Program Identifier	(AKA: UPID #):	029-00-01-11-01-1180-00

Description of System/ Application/ Program:	The VistA-Legacy system is the software platform and hardware infrastructure (associated with clinical operations) on which the VHA health care facilities operate their software applications and support for E-Government initiatives. It includes the computer equipment associated with clinical operations and the employees necessary to operate the system. VistA-Legacy is a client-server system. It links the facility computer network to over 100 applications and databases. The VistA-Legacy system supports IT services across the VA organization. At the Alaska VA Healthcare System, this includes a main outpatient facility, domiciliary, and DoD Joint Venture (Elmendorf AFB) patient care at in Anchorage, and 3 community based outpatient clinics at Juneau, Wasilla and Fairbanks. The Alaska VA VistA-Legacy provides critical data that supports the delivery of healthcare to over 17,000 veterans and their dependants. Using the computer, the VA health care provider can access VistA-Legacy applications and meet a wide range of health care data needs. The VistA-Legacy system is in the mature phase (operational/maintenance) of the capital investment lifecycle. Applications within VistA support numerous areas, including medical imaging, supply management, decision support, medical research, and education. The VistA-Legacy system for Alaska is located and managed by Region 1 IT staff in Sacramento California and Denver Colorado.
Facility Name:	Alaska VA Healthcare System

Title:	Name:	Phone:	Email:
Privacy Officer:	Sandra Jennings	907 257-4753	Sandra.Jennings@va.gov
Information Security Officer:	Randy Jansen	907 257-5428	Randy.Jansen@va.gov
System Owner/ Chief Information Officer:	Kathy Fanning	907 257-5435	Kathy.Fanning@va.gov
Information Owner:	Alex Spector	907 257-5460	Alexander.Spector@va.gov
Other Titles:			

Person Completing Document:	Randy Jansen	
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:	30,000 - 35,000
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.	15+ 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 2 & TAB 12. (See Comment for Definition of PII)

2. System Identification

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.	
For each applicable System(s) of Records, list:	
1. All System of Record Identifier(s) (number):	79VA19
2. Name of the System of Records:	VistA-VA
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm
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)	ALL	Will be kept confidential	Verbal & Written	Verbal & Written
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Wii be kept confidential	Verbal & Written	Verbal & Written
Service Information	ALL	Will be kept confidential	Verbal & Written	Verbal & Written
Medical Information	ALL	Confidentiality will be maintained in accordance tihe HIPAA & Privacy Act	Verbal & Written	Verbal & Written
Criminal Record Information	Electronic/File Transfer	Will be kept confidential	Verbal & Written	Verbal & Written
Guardian Information	Paper	Will be kept confidential	Verbal & Written	Verbal & Written
Education Information	N/A	N/A		
Benefit Information	ALL	Will be kept confidential	Verbal & Written	Verbal & Written
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	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	
Service Information	Yes	Veteran	Mandatory	
Medical Information	Yes	Veteran	Mandatory	
Criminal Record Information	No			
Guardian Information	Yes	Veteran	Mandatory	
Education Information	No			
Benefit Information	Yes	VA Files / Databases (Identify file)	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	Alaska VA Healthcare System	Yes	Medical and benefits information	Both PII & PHI	VA Handbook 1605.1
Other Veteran Organization	Alaska VA Regional Office	Yes	Medical and benefits information	Both PII & PHI	VA Handbook 1605.1
Other Federal Government Agency	Elmendorf Military Joint Base	Yes	Medical information	Both PII & PHI	VA Handbook 1605.1
State Government Agency		No			
Local Government Agency		No			
Research Entity		No			
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system? Yes

Please enter the name of the system: Health Eligibility Center (VA)

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:
- [x] 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

if yes, please check all that apply:
- [ ] Drug/Alcohol Counseling
- [ ] Mental Health
- [ ] HIV
- [ ] Research
- [ ] Sickle Cell
- [ ] 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: We follow HIPAA and 1605.2 regarding minimal necessary collection of data.

How is data checked for completeness?

Answer: Patient and staff review, compare and update current information in the computer.

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

Answer: Clinical data is never removed. Administrative data is updated with every patient encounter.

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

Answer: Accuracy of new data collected and is verified by patient and computer files.

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

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

Answer: Survivor benefits

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

Answer: Electronic final version is destroyed/deleted 75 years after the last episode of patient care as instructed in VA RCS 10-1, Item XLIII 2.b (Page 190) and in the local policy based on 6500 handbook.

Where are these procedures documented?

Answer: VA Handbook 6500 and RCS 10-1

How are data retention procedures enforced?

Answer: Records management personnel follow RCS 10-1, page 8.

Has the retention schedule been approved by the National Archives and Records Administration (NARA) Yes

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

Answer:

(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 system has been tested, certified and accredited by the VA. Last date of C&A Aug 2008.

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

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

Answer: (Other Risks) Malicious Code (could not click on to identify)

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

- ☑ Access Control
- ☑ Audit and Accountability
- ☑ Awareness and Training
- ☑ Certification and Accreditation Security Assessments
- ☑ Configuration Management
- ☑ Contingency Planning
- ☑ Identification and Authentication
- ☑ Incident Response
- ☑ Media Protection
- ☑ Personnel Security
- ☑ Physical and Environmental Protection
- ☑ 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: Additional security support provided by Region 1 IT who is the manager of the system.

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☑	The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐	The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☑	The potential impact is **high** if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐	The potential impact is **moderate** if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is **low** if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.
Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? **(Choose One)**	☑	The potential impact is **high** if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐	The potential impact is **moderate** if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is **low** if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous 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? N/A

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?

X ASISTS
X Bed Control
X CAPRI
X CMOP
X Dental
X Dietetics
X Fee Basis
GRECC
X HINQ
X IFCAP
X Imaging
X Kernal
X Kids
X Lab Service
Letterman
Library
X Mailman
X Medicine
MICOM
NDBI
X NOIS
Oncology
X PAID
X Prosthetics
X QUASER
X RPC Broker
SAGG
X Scheduling
X Social Work
X Surgery
X Toolkit
X Unwinder
X VA Fileman
X VBECS
VDEF
X VistALink

X Beneficiary Travel
X Care Management
Care Tracker
X Clinical Reminders
X CPT/ HCPCS Codes
X DRG Grouper
X DSS Extracts
X Education Tracking
X Engineering
X Event Capture
X Extensible Editor
X Health Summary
X Incident Reporting
Intake/ Output
X Integrated Billing
X Lexicon Utility
X List Manager
X Mental Health
X MyHealthEVet
X National Drug File
X Nursing Service
Occurrence Screen
X Patch Module
Patient Feedback
X Police & Security
X Problem List
X Progress Notes
X Record Tracking
X Registration
X Run Time Library
Survey Generator
X Utilization Review
X Visit Tracking
X VistALink Security
X Women's Health

X Accounts Receivable
ADP Planning (PlanMan)
Bad Code Med Admin
X Clinical Case Registries
X Clinical Procedures
X Consult/ Request Tracking
X Controlled Substances
X Credentials Tracking
X Discharge Summary
X Drug Accountability
X EEO Complaint Tracking
X Electronic Signature
X Event Driven Reporting
X External Peer Review
X Functional Independence
X Gen. Med. Rec. - I/O
X Gen. Med. Rec. - Vitals
X Generic Code Sheet
X Health Level Seven
Hospital Based Home Care
Inpatient Medications
Integrated Patient Funds
X MCCR National Database
X Minimal Patient Dataset
National Laboratory Test
X Network Health Exchange
X Outpatient Pharmacy
X Patient Data Exchange
X Patient Representative
PCE Patient/ HIS Subset
Security Suite Utility Pack
X Shift Change Handoff Tool
X Spinal Cord Dysfunction
X Text Integration Utilities
VHS & RA Tracking System
X Voluntary Timekeeping

X Adverse Reaction Tracking
X Authorization/ Subscription
X Auto Replenishment/ Ward Stock
Automated Info Collection Sys
X Automated Lab Instruments
X Automated Med Info Exchange
X Capacity Management - RUM
X Capacity Management Tools
X Clinical Info Resource Network
Clinical Monitoring System
Enrollment Application System
X Equipment/ Turn-in Request
Gen. Med.Rec. - Generator
X Health Data and Informatics
X ICR - Immunology Case Registry
X Income Verification Match
X Incomplete Records Tracking
Interim Mangement Support
X Master Patient Index VistA
Missing Patient Reg (Original) A4EL
X Order Entry/ Results Reporting
X PCE Patient Care Encounter
X Pharmacy Benefits Mangement
X Pharmacy Data Management
X Pharmacy National Database
X Pharmacy Prescription Practice
X Quality Assurance Integration
Quality Improvement Checklist
X Radiology/ Nuclear Medicine
X Release of Information - DSSI
X Remote Order/ Entry System
X Utility Management Rollup
CA Vertified Components - DSSI
X Vendor - Document Storage Sys
X Visual Impairment Service Team ANRV
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	X	Enterprise Terminology Server & VHA Enterprise Terminology Services		RALS
	Administrative Data Repository (ADR)		ePROMISE	X	Remedy Application
	ADT		EYECAP	X	SAN
X	Agent Cashier		Financial and Accounting System (FAS)		Scanning Exam and Evaluation System
	Air Fortress	X	Financial Management System	X	Sentillion
X	Auto Instrument		Genesys		Stellant
	Automated Access Request		Health Summary Contingency		Stentor
	BDN 301		ICB	X	Tracking Continuing Education
X	Bed Board Management System		KOWA	X	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
X	Clinical Data Repository/Health Data Repository		Microsoft Exchange E-mail System		VHAHUNAPP1
X	Combat Veteran Outreach		Military/Vet Eye Injury Registry		VHAHUNFPC1
	Committee on Waiver and Compromises	X	Mumps AudioFAX	X	VISTA RAD
	CP&E		NOAHLINK		Whiteboard
X	Crystal Reports Enterprise		Omnicell		
X	Data Innovations		Onvicord (VLOG)		
	DELIVEREX		Optifill		

	DICTATION-Power Scribe		P2000 ROBOT
X	DRM Plus	X	PACS database
	DSIT		Personal Computer Generated Letters
X	DSS Quadramed	X	PICIS OR
	EDS Whiteboard (AVJED)		PIV Systems
X	EKG System	X	Q-Matic
X	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 provi 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 1>VHA>VISN 20>Alaska HCS (Anchorage)>Vista-VMS

Title:	Name:	Phone:	Email:
Privacy Officer:	Sandra Jennings	907 257-4753	Sandra.Jennings@va.gov
Digital Signature Block			
Information Security Officer:	Randy Jansen	907 257-5428	Randy.Jansen@va.gov
Digital Signature Block			
System Owner/ Chief Information Officer:	Kathy Fanning	907 257-5435	Kathy.Fanning@va.gov
Digital Signature Block			
Information Owner:	Alex Spector	907 257-5460	Alexander.Spector@va.gov
Digital Signature Block			
Other Titles:	0	0	0
Digital Signature Block			

Date of Report:	1/28/11
OMB Unique Project Identifier	029-00-01-11-01-1180-00
Project Name	REGION 1>VHA>VISN 20>Alaska HCS (Anchorage)>Vista-VMS