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 submission.

Program or System Name: REGION 1>VHA> VISN 20>BOISE VETERANS AFFAIRS MEDICAL CENTER>VISTA-VMS CACHE
OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-01-11-01-1180-00

Description of System/ Application/ Program: Each VA medical center uses VistA(formerly DHCP, Decentralized Hospital Computer System), an integrated hospital information system. DHCP was an M-based internally developed portfolio and VistA encompasses DHCP and a variety of other clinical and administrative applications, some on single-use platforms. The VistA system is comprised of: InterSystems Cache on VMS (VMS/Cache) and Intersystems Cache on Redhat Linux (Linux/Cache).

Facility Name: Boise Veterans Affairs Medical Center

Title:	Name:	Phone:	Email:
Privacy Officer:	Patricia A. Smith, RHIA	208-422-1031	patricia.smith6@va.gov
Information Security Officer:	Jim Hall, CSP	208-422-1560	jim.hall2@va.gov
System Owner/ Chief Information Officer:	Mark Cecil, Acting FCIO/VISN 20 CIO	360-619-5961	mark.cecil@va.gov
Information Owner:			
Other Titles:			
Person Completing Document:	Patricia A. Smith, RHIA	208-422-1031	patricia.smith6@va.gov
Other Titles: VistA Programmer	Cindy Seburn	208-422-1153	cindy.seburn@va.gov

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY): 07/2008
Date Approval To Operate Expires: 08/21/2011

What specific legal authorities authorize this program or system:	38 USC 7301(a)
What is the expected number of individuals that will have their PII stored in this system:	96,000
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.	01/1982
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes
If No, please explain: NA	
Has a PIA been completed within the last three years?	Yes

Date of Report (MM/YYYY): 03/2011

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): NA

(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):	79VA19
2. Name of the System of Records:	Veterans Health Information Systems and Technology Architecture (VistA) Records - VA
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	http://www.rms.oit.va.gov/SOR Records.asp
Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?	Yes
Does the System of Records Notice require modification or updating?	Yes
	(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	For Treatment Purposes	Verbal & Written	Verbal & Written
Family Relation (spouse, children, parents, grandparents, etc)	ALL	For Treatment Purposes	Verbal & Written	Verbal & Written
Service Information	ALL	For Eligibility and Benefit Purposes	Verbal & Written	Verbal & Written
Medical Information	ALL	For Treatment Purposes	Verbal & Written	Verbal & Written
Criminal Record Information	VA File Database	For Eligibility and Benefit Purposes	Verbal & Written	Verbal & Written
Guardian Information	ALL	For Treatment and Confidentiality	Verbal & Written	Verbal & Written
Education Information	ALL	For Demographic Purposes	Verbal & Written	Verbal & Written
Benefit Information	ALL	For Treatment and Eligibility	Verbal & Written	Verbal & Written
Other (Explain)	N/A			

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	VA Files / Databases (Identify file)	Voluntary	Written from HEC
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Voluntary	Written from HEC
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory	Written from HEC
Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory	Written from HEC
Criminal Record Information	No	VA Files / Databases (Identify file)	Voluntary	N/A
Guardian Information	Yes	VA Files / Databases (Identify file)	Mandatory	Written from HEC
Education Information	No	VA Files / Databases (Identify file)	Voluntary	N/A
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	Written from HEC
Other (Explain)	No			
Other (Explain)	No			
Other (Explain)	No			

(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	DOD	Yes	Treatment Purposes	Both PII & PHI	Not applicable. No release
Other Veteran Organization	VSO	No	Eligibility	Both PII & PHI	Privacy Act, VA Form 10-5345. VHA Handbook 1601.1, 15. Processing a Request
Other Federal Government Agency	Remote Data Limited	Yes	Eligibility	Both PII & PHI	Privacy Act, VA Form 10-5345. VHA Handbook 1605.1
State Government Agency	Health, Law Enforcement	No	Public Health and Safety	Both PII & PHI	Standing Letter, VHA Handbook 1605.1
Local Government Agency	Health, Law Enforcement	No	Public Health and Safety	Both PII & PHI	Standing Letter, VHA Handbook 1605.1
Research Entity	NA-All employees or WOC		NA		NA
Other Project / System	NA	No	NA	N/A	NA
Other Project / System	NA	No	NA	N/A	NA
Other Project / System	NA	No	NA	N/A	NA

(FY 2011) PIA: Access to Records

Does the system gather information from another system?				No
Please enter the name of the system:	NA			
Per responses in Tab 4, does the system gather information from an individual?				Yes
If information is gathered from an individual, is the information provided:	☑ Through a Written Request ☑ Submitted in Person ☑ Online via Electronic Form	Yes	All Boxes Apply	
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:

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

All Boxes Apply

Describe process for authorizing access to this data.

Answer: Released per 38 USC 7332, Request for and consent for Release of Medical Records (VA Form 10-5345)

(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: NA

Explain how collected data are limited to required elements:

Answer: Indexing

How is data checked for completeness?

Answer: Quality Control

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

Answer: Ongoing updating with each Veteran contact.

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

Answer: Verify with Veterans, signed and authenticated by provider, signature blocks

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

Answer: NA

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: 75 years

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

Answer: Information is required for treatment, payment, and health care operations

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

Answer: VA Handbook 6300.1, pgs 16-18 Records Disposition Schedule. Item 4 'Destroy & document the destruction of records which have reached their statutory limitations.

Where are these procedures documented?

Answer: VA Handbook 6300, VA Handbook 6300.1, Records Control Schedule 10-1, 36 CFR 1234, Medical Center Policies

How are data retention procedures enforced?

Answer: All VHA employees are responsible to ensure that records are created, maintained, protected and disposed of in accordance with NARA. This facility has a Records Manager and Service liaisons to provide guidance and training and oversee the program.

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: Yes

(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: NA

(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: NA

Is adequate physical security in place to protect against unauthorized access?	Yes

If 'No' please describe why:
Answer: NA

Explain how the project meets IT security requirements and procedures required by federal law.
Answer: The System is regulated per VA Handbook 6500 requirements

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

- [x] Air Conditioning Failure
- [x] Chemical/Biological Contamination
- [x] Blackmail
- [x] Bomb Threats
- [x] 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
- [x] Earthquakes
- [x] Eavesdropping/Interception
- [x] Errors (Configuration and Data Entry)
- [x] Fire (False Alarm, Major, and Minor)
- [x] Flooding/Water Damage
- [x] Fraud/Embezzlement
- [x] Hardware Failure
- [x] Identity Theft
- [x] Malicious Code
- [x] Power Loss
- [x] Sabotage/Terrorism
- [x] Storms/Hurricanes
- [x] 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: Controls in place are sufficient for the protection of the information

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] 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)**	[x] 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)**	[x] 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? NA

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 Beneficiary Travel	X Accounts Receivable	X Adverse Reaction Tracking
X Bed Control	X Care Management	X ADP Planning (PlanMan)	X Authorization/ Subscription
X CAPRI	Care Tracker	X Bad Code Med Admin	X Auto Replenishment/ Ward Stock
X CMOP	X Clinical Reminders	X Clinical Case Registries	X Automated Info Collection Sys
X Dental	X CPT/ HCPCS Codes	X Clinical Procedures	X Automated Lab Instruments
X Dietetics	X DRG Grouper	X Consult/ Request Tracking	X Automated Med Info Exchange
X Fee Basis	X DSS Extracts	X Controlled Substances	X Capacity Management - RUM
GRECC	X Education Tracking	X Credentials Tracking	X Capacity Management Tools
X HINQ	X Engineering	X Discharge Summary	X Clinical Info Resource Network
X IFCAP	X Event Capture	X Drug Accountability	X Clinical Monitoring System
X Imaging	X Extensible Editor	X EEO Complaint Tracking	X Enrollment Application System
X Kernal	X Health Summary	X Electronic Signature	X Equipment/ Turn-in Request
X Kids	X Incident Reporting	X Event Driven Reporting	X Gen. Med.Rec. - Generator
X Lab Service	X Intake/ Output	X External Peer Review	X Health Data and Informatics
Letterman	X Integrated Billing	X Functional Independence	X ICR - Immunology Case Registry
X Library	X Lexicon Utility	X Gen. Med. Rec. - I/O	X Income Verification Match
X Mailman	X List Manager	X Gen. Med. Rec. - Vitals	X Incomplete Records Tracking
X Medicine	X Mental Health	X Generic Code Sheet	X Interim Mangement Support
MICOM	X MyHealthEVet	X Health Level Seven	X Master Patient Index VistA
X NDBI	X National Drug File	X Hospital Based Home Care	X Missing Patient Reg (Original) A4EL
NOIS	X Nursing Service	X Inpatient Medications	X Order Entry/ Results Reporting
X Oncology	X Occurrence Screen	X Integrated Patient Funds	X PCE Patient Care Encounter
X PAID	X Patch Module	X MCCR National Database	X Pharmacy Benefits Mangement
X Prosthetics	X Patient Feedback	X Minimal Patient Dataset	X Pharmacy Data Management
X QUASER	X Police & Security	X National Laboratory Test	X Pharmacy National Database
X RPC Broker	X Problem List	X Network Health Exchange	X Pharmacy Prescription Practice
X SAGG	X Progress Notes	X Outpatient Pharmacy	X Quality Assurance Integration
X Scheduling	X Record Tracking	X Patient Data Exchange	X Quality Improvement Checklist
X Social Work	X Registration	X Patient Representative	X Radiology/ Nuclear Medicine
X Surgery	X Run Time Library	X PCE Patient/ HIS Subset	X Release of Information - DSSI
X Toolkit	X Survey Generator	Security Suite Utility Pack	X Remote Order/ Entry System
X Unwinder	X Utilization Review	X Shift Change Handoff Tool	X Utility Management Rollup
X VA Fileman	X Visit Tracking	X Spinal Cord Dysfunction	CA Vertified Components - DSSI
X VBECS	X VistALink Security	X Text Integration Utilities	X Vendor - Document Storage Sys
X VDEF	X Women's Health	X VHS & RA Tracking System	X Visual Impairment Service Team ANRV
X VistALink		X Voluntary Timekeeping	X 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	Automated Medical Information System (AMIS), same as Veteran Workload Management(VWM)
Description	Generic Code Sheets are generated to download statistical information into AMIS/VWM for workload. Statistics are drawn from PII information but reports are only statistics. It is collected and displayed in national report websites (such as KLF/VSSC). AMIS Website: http://vaww.aac.va.gov/vwm/
Comments	Suggest that AMIS/VWM be added to the checklist above or at least next to Generic Code Sheets
Is PII collected by this minor application?	
Does this minor application store PII?	
If yes, where?	NA
Who has access to this data?	Employees that are responsible for reporting required programs (Adult Day Care-Fee Basis, state home, inpatient, C&P).

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
X	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
X	Data Innovations
	DELIVEREX
X	DICTATION-Power Scribe
X	DRM Plus
	DSIT
X	DSS Quadramed
	EDS Whiteboard (AVJED)
	EKG System
	Embedded Fragment Registry
	ENDSOFT
X	Enterprise Terminology Server & VHA Enterprise Terminology Services
X	ePROMISE
	EYECAP
	Financial and Accounting System (FAS)
X	Financial Management System
	Genesys
	Health Summary Contingency
X	ICB
	KOWA
	Lynx Duress Alarm
	MHTP
X	Microsoft Active Directory
X	Microsoft Exchange E-mail System
	Military/Vet Eye Injury Registry
X	Mumps AudioFAX
	NOAHLINK
X	Omnicell
	Onvicord (VLOG)
	Optifill
X	P2000 ROBOT
	PACS database
	Personal Computer Generated Letters
	PICIS OR
	PIV Systems
	Q-Matic
	QMSI Prescription Processing
	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

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?
cess to this data?

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

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

(FY 2011) PIA: Final Signatures

Facility Name: VISN 20>BOISE VETERANS AFFAIRS MEDICAL CENTER>VISTA-VMS CACHE

Title:	Name:	Phone:	Email:
Privacy Officer:	Patricia A. Smith, RHIA	208-422-1031	patricia.smith6@va.gov
Information Security Officer:	Jim Hall, CSP	208-422-1560	jim.hall2@va.gov
System Owner/ Chief Information Officer:	Mark Cecil, Acting FCIO/VISN 20 CIO	360-619-5961	mark.cecil@va.gov
Information Owner:	NA		
Facility VISTA IT	Cindy Seburn	208-422-1153	cindy.seburn@va.gov

Date of Report:	05/2011
OMB Unique Project Identifier	029-00-01-11-01-1180-00
Project Name	VISN 20>BOISE VETERANS AFFAIRS MEDICAL CENTER>VISTA-VMS CACHE