

Welcome to the PIA for FY 2010!

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. More information can be found by reading VA 6508.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vawww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the Privacy Impact Assessment Handbook 6202.2 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 Handbook 6202.2.
- 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 Handbook 6202.2 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

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 an individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirectly identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

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.

(FY 2010) PIA: System Identification

Program or System Name: OM>FSC>DMS

OMB Unique System / Application / Program Identifier (AKA: UPID #): None

Description of System / Application / Program: The DMS is a high volume system explicitly designed for the complex and diverse VA FSC DMS document processing and management requirements. Capabilities provided with the current version of the ViewStar software include remote access to DMS utilizing the Intranet. All documentation for current applications, such as invoices, purchase orders, receiving reports, credit card bills, inquiries, travel data, etc., is received at this site and entered into DMS for processing. DMS has extensively reduced the need for the VA FSC staff to handle paper and has supplied the efficient electronic distribution of information to specific VA FSC document processing functional areas.

Facility Name:	Financial Services Center		
Title:	Name:	Phone:	Email:
Privacy Officer:	Cathy Brean	512-460-5175	cathy.brean@va.gov
Information Security Officer:	Krystal Johle	512-460-5043	krystal.johle@va.gov
Chief Information Officer:	Larry Sherman	512-460-5300	larry.sherman@va.gov

Person Completing Document:	Clint Loeser	512-460-5019	clint.loeser@va.gov
Other Titles:	Terry Riffel	512-460-5100	terry.riffel@va.gov
Other Titles:	Ed Niedzielski	512-460-5207	edward.niedzielski@va.gov
Other Titles:	N/A		
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	06/2009		
Date Approval To Operate Expires:	Aug-11		
What specific legal authorities authorize this program or system:	Budgeting and Accounting Act of 1950 and General Accounting Office, Title 8, Chapter 3.		
What is the expected number of individuals that will have their PII stored in this system:	900,000		
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.	Operational for 16 years		
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes		
If No, please explain:	N/A		
Has a PIA been completed within the last three years?	Yes		
Date of Report (MM/YYYY):	01/2010		

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?

- 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 skip to TAB 12. (See Comment for Definition of PII)

(FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?

Yes

if the answer above is no, please skip to row 16.

For each applicable System(s) of Records, list:

1. All System of Record Identifier(s) (number):

13VA047

2. Name of the System of Records:

Individuals Submitting Invoices-Vouchers For
Payment-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/13VA047.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?

No

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 2010) 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)	Electronic/File Transfer	Information collected is used for payments with an addendum record that contains payment-related information.	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	N/A			
Service Information	N/A			
Medical Information	N/A			
Criminal Record Information				
Guardian Information	N/A			
Education Information	N/A			
Benefit Information	N/A			
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	
Family Relation (spouse, children, parents, grandparents, etc)	No			
Service Information	No			
Medical Information	Yes	Other (Explain)	Voluntary	Vendors may attach PHI data to submitted invoices to describe health services provided.
Criminal Record Information	No			

Guardian Information	No
Education Information	No
Benefit Information	No
Other (Explain)	No
Other (Explain)	No
Other (Explain)	No

(FY 2010) 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	VHA	Yes	This system maintains records of vendors and others to whom VA makes payments as the result of invoices, vouchers, and other documentary requests for payment, and payment history records. VA makes payments through the Department of the Treasury. A variety of automated applications are utilized to support electronic orders, invoices, receiving reports, and payments. Records include, but are not limited to, billing and payment information, purchase orders, vendor invoices, checks, reimbursement documents, transaction amounts, goods and services descriptions.	Both PII & PHI	13VA047 and Privacy Act
Other Veteran Organization		No	N/A	N/A	N/A

Other Federal Government Agency	Treasury and IRS	No	Transfer payment information necessary to complete payment of claims and to furnish income data Form 1099 to the Treasury Department in order to effect payment of claims to vendors and to furnish income information.	PII	13VA047 and Privacy Act
---------------------------------	------------------	----	---	-----	-------------------------

State Government Agency	N/A
Local Government Agency	N/A
Research Entity	N/A
Other Project / System	N/A
Other Project / System	N/A
Other Project / System	N/A

(FY 2010) PIA: Access to Records

Does the system gather information from another system? Yes
 Please enter the name of the system: Sequel Invoice Database and Electronic Data Interchange

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

Is there a contingency plan in place to process information when the system is down? Yes

(FY 2010) 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: N/A

(FY 2010) 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: N/A

Explain how collected data are limited to required elements:

Answer: Only necessary fields required are manually input into DMS. Complete image resides within the system, but is not used to make payment.

How is data checked for completeness?

Answer: Edit checks are conducted on every incoming invoice in the system. Exceptions can be granted or invoice will be returned to submitter to provide more information.

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

Answer: It's up to the individual vendor Payee/Company to provide up-to-date information.

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

Answer: Vendor information is authenticated with the IRS to ensure Tax Identification Number is valid and applicable to vendor.

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

Answer: None

(FY 2010) PIA: Retention & Disposal

What is the data retention period?

Answer: Records are retained on tape and electronic media for 6 years and 3 months as required by GRS 6, Item 1a.

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

Answer: Governed by General Accounting Office Regulations which require retention for records created prior to July 2, 1975: 10 years and 3 months after the period of the account; records created on and after July 2, 1975: 6 years and 3 months after the period of the account.

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

Answer: We have developed file plans for the services that use this system and are currently developing SOPs on how to automate the destruction of media at the appropriate time based on published NARA and VA instructions.

Where are these procedures documented?

Answer: We are currently working on the SOPs and they will reside with system users and records custodian that when complete, will provide detailed instructions on how to properly destroy both hard copy and electronic copy.

How are data retention procedures enforced?

Answer: Applying correct NARA GRS. We are finalizing procedures to classify categories of documents with appropriate disposition. Once completed records that have met their retention period will automatically be flagged for disposition.

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: MP-4, Part X VA GRS for Office of Budge and Finance is also the approved NARA retention authority for DMS

(FY 2010) 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 2010) 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 DMS has been operational for over 15 years. The necessary restrictions and security controls were part of the original design and were addressed during any system upgrades to maintain the confidentiality, integrity, and availability of the system. Security controls are regularly audited to ensure said controls are implemented and operating as intended. The data found in this system can only be accessed by individuals with approved access and those personnel must complete the required background investigations and annual security and privacy awareness training prior to gaining access to the system.

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

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

Answer: (Other Risks)

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

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

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: Reconsideration of collection information in DMS, additional security controls to mitigate the risks listed above and proper retention of data.

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 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.

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 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.

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 2010) PIA: Additional Comments

Add any additional comments on this tab for any question in the form you want to comment on.
Please indicate the question you are responding to and then add your comments.

(FY 2010) PIA: VBA Minor Applications

Explain what minor application that are associated with your installation? *(Check all that apply)*

Records Locator System	Education Training Website	Appraisal System
Veterans Assistance Discharge System (VADS)	VR&E Training Website	Web Electronic Lender Identification
LGY Processing	VA Reserve Educational Assistance Program	CONDO PUD Builder
Loan Service and Claims	Web Automated Verification of Enrollment	Centralized Property Tracking System
LGY Home Loans	Right Now Web	Electronic Appraisal System
Search Participant Profile (SPP)	VA Online Certification of Enrollment (VA-ONCE)	Web LGY
Control of Veterans Records (COVERS)	Automated Folder Processing System (AFPS)	Access Manager
SHARE	Personal Computer Generated Letters (PCGL)	SAHSHA
Modern Awards Process Development (MAP-D)	Personnel Information Exchange System (PIES)	VBA Data Warehouse
Rating Board Automation 2000 (RBA2000)	Rating Board Automation 2000 (RBA2000)	Distribution of Operational Resources (DOOR)
State of Case/Supplemental (SOC/SSOC)	SHARE	Enterprise Wireless Messaging System (Blackberry)
Awards	State Benefits Reference System	VBA Enterprise Messaging System
Financial and Accounting System (FAS)	Training and Performance Support System (TPSS)	LGY Centralized Fax System
Eligibility Verification Report (EVR)	Veterans Appeals Control and Locator System (VACOLS)	Review of Quality (ROQ)
Automated Medical Information System (AMIS)290	Veterans On-Line Applications (VONAPP)	Automated Sales Reporting (ASR)
Web Automated Reference Material System (WARMS)	Automated Medical Information Exchange II (AIME II)	Electronic Card System (ECS)
Automated Standardized Performance Elements Nationwide (ASPEN)	Committee on Waivers and Compromises (COWC)	Electronic Payroll Deduction (EPD)
Inquiry Routing Information System (IRIS)	Common Security User Manager (CSUM)	Financial Management Information System (FMI)
National Silent Monitoring (NSM)	Compensation and Pension (C&P) Record Interchange (CAPRI)	Purchase Order Management System (POMS)
Web Service Medical Records (WebSMR)	Control of Veterans Records (COVERS)	Veterans Canteen Web
Systematic Technical Accuracy Review (STAR)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)	Inventory Management System (IMS)
Fiduciary STAR Case Review	Fiduciary Beneficiary System (FBS)	Synquest
Veterans Exam Request Info System (VERIS)	Hearing Officer Letters and Reports System (HOLAR)	RAI/MDS
Web Automated Folder Processing System (WAFPS)	Inforce	ASSISTS
Courseware Delivery System (CDS)	Awards	MUSE
Electronic Performance Support System (EPSS)	Actuarial	Bbraun (CP Hemo)
Veterans Service Representative (VSR) Advisor	Insurance Self Service	VIC
Loan Guaranty Training Website	Insurance Unclaimed Liabilities	BCMA Contingency Machines
C&P Training Website	Insurance Online	Script Pro

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.

Minor app #1	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?		

Minor app #2	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?		

Minor app #3	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?		

Baker System	Veterans Assistance Discharge System (VADS)
Dental Records Manager	VBA Training Academy
Sidexis	Veterans Service Network (VETSNET)
Priv Plus	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
Mental Health Assistant	BIRLS
Telecare Record Manager	Centralized Accounts Receivable System (CARS)
Omicell	Compensation & Pension (C&P)
Powerscribe Dictation System	Corporate Database
EndoSoft	Control of Veterans Records (COVERS)
Compensation and Pension (C&P)	Data Warehouse
Montgomery GI Bill	INS - BIRLS
Vocational Rehabilitation & Employment (VR&E) CH 31	Mobilization
Post Vietnam Era educational Program (VEAP) CH 32	Master Veterans Record (MVR)
Spinal Bifida Program Ch 18	BDN Payment History
C&P Payment System	
Survivors and Dependents Education Assistance CH 35	
Reinstatement Entitlement Program for Survivors (REAPS)	
Educational Assistance for Members of the Selected Reserve Program CH 1606	
Reserve Educational Assistance Program CH 1607	
Compensation & Pension Training Website	
Web-Enabled Approval Management System (WEAMS)	
FOCAS	
Work Study Management System (WSMS)	
Benefits Delivery Network (BDN)	
Personnel and Accounting Integrated Data and Fee Basis (PAID)	
Personnel Information Exchange System (PIES)	
Rating Board Automation 2000 (RBA2000)	
SHARE	
Service Member Records Tracking System	

(FY 2010) PIA: VISTA Minor Applications

Explain what minor application that are associated with your installation? *(Check all that apply)*

ACCOUNTS RECEIVABLE	DRUG ACCOUNTABILITY	INPATIENT MEDICATIONS
ADP PLANNING (PLANMAN) ADVERSE REACTION TRACKING ASISTS	DSS EXTRACTS EDUCATION TRACKING EEO COMPLAINT TRACKING	INTAKE/OUTPUT INTEGRATED BILLING INTEGRATED PATIENT FUNDS
AUTHORIZATION/SUBSCRIPTION	ELECTRONIC SIGNATURE	INTERIM MANAGEMENT SUPPORT
AUTO REPLENISHMENT/WARD STOCK	ENGINEERING	KERNEL
AUTOMATED INFO COLLECTION SYS	ENROLLMENT APPLICATION SYSTEM	KIDS
AUTOMATED LAB INSTRUMENTS	EQUIPMENT/TURN-IN REQUEST	LAB SERVICE
AUTOMATED MED INFO EXCHANGE	EVENT CAPTURE	LETTERMAN
BAR CODE MED ADMIN	EVENT DRIVEN REPORTING	LEXICON UTILITY
BED CONTROL	EXTENSIBLE EDITOR	LIBRARY
BENEFICIARY TRAVEL	EXTERNAL PEER REVIEW	LIST MANAGER
CAPACITY MANAGEMENT - RUM	FEE BASIS	MAILMAN
CAPRI	FUNCTIONAL INDEPENDENCE	MASTER PATIENT INDEX VISTA
CAPACITY MANAGEMENT TOOLS	GEN. MED. REC. - GENERATOR	MCCR NATIONAL DATABASE
CARE MANAGEMENT CLINICAL CASE REGISTRIES	GEN. MED. REC. - I/O GEN. MED. REC. - VITALS	MEDICINE MENTAL HEALTH
CLINICAL INFO RESOURCE NETWORK	GENERIC CODE SHEET	MICOM
CLINICAL MONITORING SYSTEM	GRECC	MINIMAL PATIENT DATASET
CLINICAL PROCEDURES	HEALTH DATA & INFORMATICS	MYHEALTHVET
CLINICAL REMINDERS	HEALTH LEVEL SEVEN	Missing Patient Reg (Original) A4EL
CMOP	HEALTH SUMMARY	NATIONAL DRUG FILE
CONSULT/REQUEST TRACKING	HINQ	NATIONAL LABORATORY TEST
CONTROLLED SUBSTANCES	HOSPITAL BASED HOME CARE	NDBI
CPT/HCPCS CODES	ICR - IMMUNOLOGY CASE REGISTRY	NETWORK HEALTH EXCHANGE
CREDENTIALS TRACKING DENTAL DIETETICS	IFCAP IMAGING INCIDENT REPORTING	NOIS NURSING SERVICE OCCURRENCE SCREEN
DISCHARGE SUMMARY	INCOME VERIFICATION MATCH	ONCOLOGY
DRG GROUPER	INCOMPLETE RECORDS TRACKING	ORDER ENTRY/RESULTS REPORTING

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.

Minor app #1	Name		Description	Comments
		<input type="checkbox"/>	Is PII collected by this min or application?	
		<input type="checkbox"/>	Does this minor application store PII?	
			If yes, where?	
		Who has access to this data?		

Minor app #2	Name		Description	Comments
		<input type="checkbox"/>	Is PII collected by this min or application?	
		<input type="checkbox"/>	Does this minor application store PII?	
			If yes, where?	
		Who has access to this data?		

Minor app #3	Name		Description	Comments
		<input type="checkbox"/>	Is PII collected by this min or application?	
		<input type="checkbox"/>	Does this minor application store PII?	
			If yes, where?	
		Who has access to this data?		

OUTPATIENT PHARMACY	SOCIAL WORK
PAID PATCH MODULE PATIENT DATA EXCHANGE	SPINAL CORD DYSFUNCTION SURGERY SURVEY GENERATOR
PATIENT FEEDBACK	TEXT INTEGRATION UTILITIES
PATIENT REPRESENTATIVE	TOOLKIT
PCE PATIENT CARE ENCOUNTER PCE PATIENT/IHS SUBSET	UNWINDER UTILIZATION MANAGEMENT ROLLUP
PHARMACY BENEFITS MANAGEMENT PHARMACY DATA MANAGEMENT PHARMACY NATIONAL DATABASE PHARMACY PRESCRIPTION PRACTICE POLICE & SECURITY	UTILIZATION REVIEW VA CERTIFIED COMPONENTS - DSSI VA FILEMAN VBECs VDEF
PROBLEM LIST	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES	VHS&RA ADP TRACKING SYSTEM
PROSTHETICS QUALITY ASSURANCE INTEGRATION QUALITY IMPROVEMENT CHECKLIST QUASAR	VISIT TRACKING VISTALINK VISTALINK SECURITY VISUAL IMPAIRMENT SERVICE TEAM ANRV
RADIOLOGY/NUCLEAR MEDICINE RECORD TRACKING	VOLUNTARY TIMEKEEPING VOLUNTARY TIMEKEEPING NATIONAL
REGISTRATION	WOMEN'S HEALTH
RELEASE OF INFORMATION - DSSI	CARE TRACKER
REMOTE ORDER/ENTRY SYSTEM RPC BROKER	
RUN TIME LIBRARY SAGG SCHEDULING	
SECURITY SUITE UTILITY PACK	
SHIFT CHANGE HANDOFF TOOL	

(FY 2010) PIA: Minor Applications

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

Minor app #1	Name		Description		Comments
		<input type="checkbox"/>	Is PII collected by this min or application?		
		<input type="checkbox"/>	Does this minor application store PII?		
			If yes, where?		
		Who has access to this data?			

Minor app #2	Name		Description		Comments
		<input type="checkbox"/>	Is PII collected by this min or application?		
		<input type="checkbox"/>	Does this minor application store PII?		
			If yes, where?		
		Who has access to this data?			

Minor app #3	Name		Description		Comments
		<input type="checkbox"/>	Is PII collected by this min or application?		
		<input type="checkbox"/>	Does this minor application store PII?		
			If yes, where?		
		Who has access to this data?			

(FY 2010) PIA: Final Signatures

Facility Name: Financial Services Center

Title:	Name:	Phone:	Email:
Privacy Officer:	Cathy Brean	512-460-5175	cathy.brean@va.gov
Digital Signature Block			
Information Security Officer:	Krystal Johle	512-460-5043	krystal.johle@va.gov
Digital Signature Block			
Chief Information Officer:	Larry Sherman	512-460-5300	larry.sherman@va.gov
Digital Signature Block			
Person Completing Document:	Clint Loeser	512-460-5019	clint.loeser@va.gov
Digital Signature Block			
System / Application / Program Manager:	Terry Riffel	512-460-5100	terry.riffel@va.gov
Digital Signature Block			

Date of Report: 1/1/2010
 OMB Unique Project Identifier: None
 Project Name: OM>FSC>DMS