

## (FY 2012) PIA: System Identification

Program or System Name: Development>CDCO > AITC > VA > National Utilization Management Integration (NUMI)  
 OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-01-11-01-5113-00  
 Description of System/ Application/ Program: The NUMI application is a web-based solution that automates utilization review assessment and outcomes. The Utilization Management (UM) Process is a tool used to help ensure that patients are receiving the right care, at the right time, and in the right place. UM is both, a quality and efficiency tool, as it is used to move patients efficiently through the VA system to maximize use of resources. UM reviewers assess patient admissions and hospital stay-days using standardized objective evidence-based clinical criteria to determine whether patients meet criteria for acute hospital care.

Facility Name:	Austin Information Technology Center (AITC)		
Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	512-326-6217	<a href="mailto:Amy.Howe1@va.gov">Amy.Howe1@va.gov</a>
Information Security Officer:	Thomas Wolf	512-326-6137	<a href="mailto:thomas.wolf5@va.gov">thomas.wolf5@va.gov</a>
System Owner	John Rucker	512-326-6422	<a href="mailto:John.Rucker@va.gov">John.Rucker@va.gov</a>
Other Titles:			
Other Titles:			

Person Completing Document:  
 Other Titles:  
 Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY) N/A  
 Date Approval To Operate Expires: N/A

What specific legal authorities authorize this program or system? Title 38, United States Code, Section 501  
 What is the expected number of individuals that will have their PII stored in this system: 800,000  
 Identify what stage the System / Application / Program is at: Development/Acquisition  
 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. 09/2011  
 Is there an authorized change control process which documents any changes to existing applications or systems? N/A: First PIA  
 If No, please explain:  
 Has a PIA been completed within the last three years? No  
 Date of Report (MM/YYYY): 08/2011

**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?
- 2.  Does this system/application/program collect, store or disseminate the SSN?

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)**

## (FY 2012) 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):

121VA19

2. Name of the System of Records:

VA National Patient Database

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](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?

No

***(Please Select Yes/No)***

Is PII collected by paper methods?

No

Is PII collected by verbal methods?

No

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

No

Proximity and Timing: Is the privacy notice provided at the time of data collection?

No

Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

No

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

No

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

No

## (FY 2012) PIA: Notice

Please fill in each column for the data types selected.

<b>Data Type</b>	<b>Collection Method</b>	<b>What will the subjects be told about the information collection?</b>	<b>How is this message conveyed to them?</b>	<b>How is a privacy notice provided?</b>
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	VA File Database	N/A Information retrieved from another system	N/A	N/A
Family Relation (spouse, children, parents, grandparents, etc)	N/A	N/A	N/A	N/A
Service Information	N/A	N/A	N/A	N/A
Medical Information	Electronic/File Transfer	N/A Information retrieved from another system		
Criminal Record Information	N/A	N/A	N/A	N/A
Guardian Information	N/A	N/A	N/A	N/A
Education Information	N/A	N/A	N/A	N/A
Benefit Information	N/A	N/A	N/A	N/A
Other (Explain)	N/A	N/A	N/A	N/A

<b>Data Type</b>	<b>Is Data Type Stored on your system?</b>	<b>Source</b> (If requested, identify the specific file, entity and/or name of agency)	<b>Is data collection Mandatory or Voluntary?</b>	<b>Additional Comments</b>
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	VistA
Family Relation (spouse, children, parents, grandparents, etc)	No			

Service Information	No			
Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory	VistA
Criminal Record Information	No			
Guardian Information	No			
Education Information	No			
Benefit Information	No			
Other (Explain)				
Other (Explain)				
Other (Explain)				

## (FY 2012) 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	VSSC	No	See Tab 8	Both PII & PHI	See Tab 8
Other Veteran Organization	NA				
Other Federal Government Agency	NA				
State Government Agency	NA				
Local Government Agency	NA				
Research Entity	NA				
Other Project / System					
Other Project / System					
Other Project / System					

## (FY 2012) PIA: Access to Records

Does the system gather information from another system?		Yes
Please enter the name of the system:	VistA	
Per responses in Tab 4, does the system gather information from an individual?		No
If information is gathered from an individual, is the information provided:	<input type="checkbox"/> Through a Written Request <input type="checkbox"/> Submitted in Person <input type="checkbox"/> Online via Electronic Form	
Is there a contingency plan in place to process information when the system is down?		Yes

## (FY 2012) PIA: Secondary Use

Will PII data be included with any secondary use request?		No
if yes, please check all that apply:	<input type="checkbox"/> Drug/Alcohol Counseling <input type="checkbox"/> Mental Health <input type="checkbox"/> HIV <input type="checkbox"/> Research <input type="checkbox"/> Sickle Cell <input type="checkbox"/> Other (Please Explain)	

Describe process for authorizing access to this data.

Answer:

## (FY 2012) 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: MDWS Ware is an AVIVA Product that limits data by remote procedure call (PRC) calls that is established in Vista.

How is data checked for completeness?

Answer: Utilization managers at each site review the data daily.

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

Answer: Utilization managers at each site review the data daily.

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

Answer: Utilization managers at each site review the data daily.

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

Answer:

## (FY 2012) PIA: Retention & Disposal

What is the data retention period?

Would follow RCS 10-1 for current retention guidelines. Indefinitely.

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

Answer: Longitudinal analysis.

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

Answer: N/A

Where are these procedures documented?

Answer: RCS 10-1

How are data retention procedures enforced?

Answer: RCS 10-1

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 2012) 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 2012) 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: System will go through Certification and Accreditation(C&A) process and obtain an Authority to Operate(ATO).

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

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

Answer: (Other Risks)

---

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

- 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: None

---

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 2012) 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.

NUMI may eventually share information with two more systems: VMS and AVIVA.

**Tab 5, 4D & 4F** - PII, PHI and other data are pulled from VistA into the business application NUMI where the data is used to drive workflow related to Utilization Management (UM), which includes the process of ensuring that patients are receiving the right level of care. In order for a NUMI user to have access to PII through NUMI, the user must have access to VistA. Access to the NUMI software is actually obtained by authenticating into VistA. Utilization Management information gathered in NUMI is then relayed to VSSC for analysis and reporting. VSSC does not receive any PII from NUMI that it does not already get from other sources such as the CDW (Corporate Data Warehouse); however, for the purpose of relating NUMI data back to other patient information in the CDW, PII is transmitted to VSSC.

## (FY 2012) PIA: VBA Minor Applications

<b>Which of these are sub-components of your system?</b>
--

Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial	BCMA Contingency Machines	Automated Medical Information Exchange II (AIME II)
Appraisal System	Benefits Delivery Network (BDN)	Automated Medical Information System (AMIS)290
ASSISTS	Centralized Property Tracking System	Automated Standardized Performace Elements Nationwide (ASPEN)
Awards	Common Security User Manager (CSUM)	Centralized Accounts Receivable System (CARS)
Awards	Compensation and Pension (C&P)	Committee on Waivers and Compromises (COWC)
Baker System	Control of Veterans Records (COVERS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)	Control of Veterans Records (COVERS)	Compensation & Pension Training Website
BDN Payment History	Control of Veterans Records (COVERS)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
BIRLS	Courseware Delivery System (CDS)	Distribution of Operational Resources (DOOR)
C&P Payment System	Dental Records Manager	Educational Assistance for Members of the Selected Reserve Program CH 1606
C&P Training Website	Education Training Website	Electronic Performance Support System (EPSS)
CONDO PUD Builder	Electronic Appraisal System	Enterprise Wireless Messaging System (Blackberry)
Corporate Database	Electronic Card System (ECS)	Financial Management Information System (FMI)
Data Warehouse	Electronic Payroll Deduction (EPD)	Hearing Officer Letters and Reports System (HOLAR)
EndoSoft	Eligibility Verification Report (EVR)	Inquiry Routing Information System (IRIS)
FOCAS	Fiduciary Beneficiary System (FBS)	Modern Awards Process Development (MAP-D)
Inforce	Fiduciary STAR Case Review	Personnel and Accounting Integrated Data and Fee Basis (PAID)
INS - BIRLS	Financial and Accounting System (FAS)	Personal Computer Generated Letters (PCGL)
Insurance Online	Insurance Unclaimed Liabilities	Personnel Information Exchange System (PIES)
Insurance Self Service	Inventory Management System (IMS)	Personnel Information Exchange System (PIES)
LGY Home Loans	LGY Centralized Fax System	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing	Loan Service and Claims	Purchase Order Management System (POMS)
Mobilization	Loan Guaranty Training Website	Reinstatement Entitelment Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Asisstant	Service Member Records Tracking System
Omnicell	National Silent Monitoring (NSM)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Powerscribe Dictation System	Systematic Technical Accuracy Review (STAR)
RAI/MDS	Rating Board Automation 2000 (RBA2000)	Training and Performance Support System (TPSS)
Right Now Web	Rating Board Automation 2000 (RBA2000)	VA Online Certification of Enrollment (VA-ONCE)
SAHSHA	Rating Board Automation 2000 (RBA2000)	VA Reserve Educational Assistance Program
Script Pro	Records Locator System	Veterans Appeals Control and Locator System (VACOLS)
SHARE	Review of Quality (ROQ)	Veterans Assistance Discharge System (VADS)
SHARE	Search Participant Profile (SPP)	Veterans Exam Request Info System (VERIS)
SHARE	Spinal Bifida Program Ch 18	Veterans Service Representative (VSR) Advisor
Sidexis	State Benefits Reference System	Vocational Rehabilitation & Employment (VR&E) CH 31
Synquest	State of Case/Supplemental (SOC/SSOC)	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

VBA Data Warehouse  
VBA Training Academy  
Veterans Canteen Web  
VIC  
VR&E Training Website  
Web LGY

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

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

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

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

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

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

(FY 2012) PIA: VISTA Minor Applications

**Which of these are sub-components of your system?**

ASISTS	Beneficiary Travel	Accounts Receivable	Adverse Reaction Tracking
Bed Control	Care Management	ADP Planning (PlanMan)	Authorization/ Subscription
CAPRI	Care Tracker	Bad Code Med Admin	Auto Replenishment/ Ward Stock
CMOP	Clinical Reminders	Clinical Case Registries	Automated Info Collection Sys
Dental	CPT/ HCPCS Codes	Clinical Procedures	Automated Lab Instruments
Dietetics	DRG Grouper	Consult/ Request Tracking	Automated Med Info Exchange
Fee Basis	DSS Extracts	Controlled Substances	Capacity Management - RUM
GRECC	Education Tracking	Credentials Tracking	Capacity Management Tools
HINQ	Engineering	Discharge Summary	Clinical Info Resource Network
IFCAP	Event Capture	Drug Accountability	Clinical Monitoring System
Imaging	Extensible Editor	EEO Complaint Tracking	Enrollment Application System
Kernal	Health Summary	Electronic Signature	Equipment/ Turn-in Request
Kids	Incident Reporting	Event Driven Reporting	Gen. Med.Rec. - Generator
Lab Service	Intake/ Output	External Peer Review	Health Data and Informatics
Letterman	Integrated Billing	Functional Independence	ICR - Immunology Case Registry
Library	Lexicon Utility	Gen. Med. Rec. - I/O	Income Verification Match
Mailman	List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine	Mental Health	Generic Code Sheet	Interim Mangement Support
MICOM	MyHealthEVet	Health Level Seven	Master Patient Index VistA
NDBI	National Drug File	Hospital Based Home Care	Missing Patient Reg (Original) A4EL
NOIS	Nursing Service	Inpatient Medications	Order Entry/ Results Reporting
Oncology	Occurrence Screen	Integrated Patient Funds	PCE Patient Care Encounter
PAID	Patch Module	MCCR National Database	Pharmacy Benefits Mangement
Prosthetics	Patient Feedback	Minimal Patient Dataset	Pharmacy Data Management
QUASER	Police & Security	National Laboratory Test	Pharmacy National Database
RPC Broker	Problem List	Network Health Exchange	Pharmacy Prescription Practice
SAGG	Progress Notes	Outpatient Pharmacy	Quality Assurance Integration
Scheduling	Record Tracking	Patient Data Exchange	Quality Improvement Checklist
Social Work	Registration	Patient Representative	Radiology/ Nuclear Medicine
Surgery	Run Time Library	PCE Patient/ HIS Subset	Release of Information - DSSI
Toolkit	Survey Generator	Security Suite Utility Pack	Remote Order/ Entry System
Unwinder	Utilization Review	Shift Change Handoff Tool	Utility Management Rollup
VA Fileman	Visit Tracking	Spinal Cord Dysfunction	CA Verified Components - DSSI
VBECS	VistALink Security	Text Integration Utilities	Vendor - Document Storage Sys
VDEF	Women's Health	VHS & RA Tracking System	Visual Impairment Service Team ANRV
VistALink		Voluntary Timekeeping	Voluntary Timekeeping National

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

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

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

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

(FY 2012) PIA: Minor Applications

**Which of these are sub-components of your system?**

1184 Web	ENDSOFT	RAFT
A4P	Enterprise Terminology Server & VHA Enterprise Terminology Services	RALS
Administrative Data Repository (ADR)	ePROMISE	Remedy Application
ADT	EYECAP	SAN
Agent Cashier	Financial and Accounting System (FAS)	Scanning Exam and Evaluation System
Air Fortress	Financial Management System	Sentillion
Auto Instrument	Genesys	Stellant
Automated Access Request	Health Summary Contingency	Stentor
BDN 301	ICB	Tracking Continuing Education
Bed Board Management System	KOWA	Traumatic Brain Injury
Cardiff Teleform	Lynx Duress Alarm	VA Conference Room Registration VAMedSafe
Cardiology Systems (stand alone servers from the network)	MHTP	
CHECKPOINT	Microsoft Active Directory	VBA Data Warehouse
Clinical Data Repository/Health Data Repository	Microsoft Exchange E-mail System	VHAHUNAPP1 VHAHUNFPC1
Combat Veteran Outreach Committee on Waiver and Compromises	Military/Vet Eye Injury Registry	VISTA RAD
CP&E	Mumps AudioFAX	Whiteboard
Crystal Reports Enterprise	NOAHLINK	
Data Innovations	Omicell	
DELIVEREX	Onvicord (VLOG)	
DICTATION-Power Scribe	Optifill	
DRM Plus	P2000 ROBOT	
DSIT	PACS database	
DSS Quadramed	Personal Computer Generated Letters	
EDS Whiteboard (AVJED)	PICIS OR	
EKG System	PIV Systems	
Embedded Fragment Registry	Q-Matic	
	QMSI Prescription Processing	

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

Name
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 2012) PIA: Final Signatures

Facility Name: Development>CDCO > AITC > VA > National Utilization Management Integration (NUMI)

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

Privacy Officer:	Amy Howe	512-326-6217	Amy.Howe1@va.gov
------------------	----------	--------------	------------------

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

Information Security Officer:	Thomas Wolf	512-326-6137	thomas.wolf5@va.gov
-------------------------------	-------------	--------------	---------------------

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

System Owner	John Rucker	512-326-6422	John.Rucker@va.gov
--------------	-------------	--------------	--------------------

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

Other Titles:	0	0	
---------------	---	---	--

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

Other Titles:	0	0	0
---------------	---	---	---

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

Date of Report: 8/3/11

OMB Unique Project Identifier 029-00-01-11-01-5113-00

Project Name Development>CDCO > AITC > VA >  
National Utilization Management  
Integration (NUMI)

(FY 2011) PIA: Final Signatures

Facility Name:

AITC

Privacy Officer: Amy Howe

Information Security Officer: THOMAS M WOLF ISO

Digital Signature Block

512-326-6217

Amy.Howe1@va.gov

Digital Signature Block

512-326-187

Thomas.Wolf5@va.gov

System Owner/Chief Information Officer: John Rucker

Digital Signature Block

512-326-6422

John.Rucker@va.gov

Information Owner:

Digital Signature Block

Other Titles:

Digital Signature Block

Date of Report:

OMB Unique Project Identifier

Project Name