

(FY 2012) PIA: System Information		*Green Highlight = Must Answer Question		*Yellow Highlight = Required to Sign PIA	
Program or System Name (as shown in SMART):		REGION 2 > VHA > VISN 15 > Kansas City VAMC > VistA - VMS			
OMB Unique System / Application / Program Identifier (AKA: UPIID #):		029-00-01-11-01-1180-00			
Description of System/ Application/ Program : "must match what is stated in System Security Plan (SSP)"		The VistA system is the software platform and hardware infrastructure (associated with clinical operations) on which the VHA health care facilities operate their software applications and support for E-Government initiatives. It includes the computer equipment associated with clinical operations and the employees necessary to operate the system. VistA is a client-server system. It links the facility computer network to applications and databases. VistA provides critical data that supports the delivery of healthcare to veterans and their dependants. Using the computer, the VA health care provider can access VistA applications and meet a wide range of health care data needs. The VistA system operates in medical centers, ambulatory and community-based clinics, nursing homes and domiciliary. The VistA system is in the mature phase of the capital investment lifecycle.			
Facility or Program Office Name:		Kansas City, MO			
Title:		Name:		Phone:	
Privacy Officer:		Gayle Gregory		816-861-4700 x57101	
Information Security Officer:		David Collins		816-922-2038	
System Owner/Delegate:		George Parry		816-701-3048	
Chief Information Officer:		Eddie Johnson		816-861-4700 x54295	
Information Owner:					
Other Titles:					
Person Completing Document:		Sandra Hedtke		701-237-2566	
Other Titles:					
Date of Last Full Approved PIA by VACO Privacy Services: (MM/YYYY)		07/2009			
What specific legal authorities authorize this program or system:		Title 38, USC, section 7301 (a)			
What is the expected number of individuals that will have their PII stored in this system:		1,000,000+			
Identify what stage the System / Application / Program is at:		Implementation			
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.		25 years			
Is there an authorized change control process which documents any changes to existing applications or systems?		<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PIA			
If No, (Explain on Tab 8)					
Is there a contingency plan in place to process information when the system is down?		<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PIA			
Has a PIA been completed within the last three years?		<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PIA			
FISMA QUESTIONS					
1. Is this a new system?		<input type="radio"/> Yes <input checked="" type="radio"/> No			
2. Does this system contain Federal information in identifiable form?		<input checked="" type="radio"/> Yes <input type="radio"/> No			
3. Does the system include information on the public?		<input checked="" type="radio"/> Yes <input type="radio"/> No			
4. Is there a Privacy Impact Assessment (PIA) that covers this system?		<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> National Security System under 40 U.S.C. 11103, a PIA is not required for this system			
5. Is Federal-owned information in this system retrieved by name or unique		<input checked="" type="radio"/> Yes <input type="radio"/> No			
6. What is the System of Records Notice (SORN) for this system?		79VA19			
7. Has this SORN been reviewed or updated within the last three years?		Yes last year			
Date of Report (MM/YYYY):		2/2012			
Any check mark in the boxes below will require a full PIA. Please continue to the next TAB and complete the remaining questions. If there is no Personally Identifiable Information on your system, please complete TAB 2 & TAB 12. (See Comment for Definition of PII)					
<input checked="" type="checkbox"/> Have any changes been made to the system since the last PIA?					
<input type="checkbox"/> Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?					
<input checked="" type="checkbox"/> Will this system/application/program retrieve information on the basis of name, unique identifier, symbol or other PII data?					

<input checked="" type="checkbox"/> Does this system/application/program collect, store, or disseminate PII/PHI data?				
<input checked="" type="checkbox"/> Does this system/application/program collect, store or disseminate the SSN?				
Directions				

(FY 2012) PIA: System of Records

*Green Highlight = Must Answer Question

- 1. Is a SORN (System of Records Notice) Required?
- 2. Is there a SORN already in place?

Yes No Not Sure

Yes No

***If Yes, select all of the appropriate SORN number(s):
 ***If Not Sure, continue to question 3

***Click to add. Delete SORN by highlighting SORN and comma if included and press the Delete key or place focus on area to delete all SORNs.

LIST OF SORN NUMBER(S) :

79VA19

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

- 3. If records are retrieved using any of the following entities, A SORN will be required (Please check all that apply)

<input checked="" type="checkbox"/> Full Name
<input type="checkbox"/> Maiden Name
<input type="checkbox"/> Mother's Maiden Name
<input type="checkbox"/> Alias
<input checked="" type="checkbox"/> Social Security Number
<input type="checkbox"/> Passport Number
<input type="checkbox"/> Driver's License Number
<input type="checkbox"/> Taxpayer Identification Number
<input type="checkbox"/> Financial Account Number
<input type="checkbox"/> Credit Card Number
<input type="checkbox"/> Street Address
<input type="checkbox"/> Email Address
<input type="checkbox"/> Photographic Image
<input type="checkbox"/> Fingerprints
<input type="checkbox"/> Handwriting
<input type="checkbox"/> Other Biometric Data
<input type="checkbox"/> Other (Explain on Tab 8)

- 4. Based on Question 3, is a SORN required?

Yes No

Yes No

***If Yes, has the process begun to obtain/acquire a SORN

Location where the specific applicable System of Records Notice may be accessed:

http://www.rms.oit.va.gov/SOR_Records.asp

(FY 2012) PIA: Data Collection And Storage *Green Highlight = Must Answer Question

Please fill in each column for the data types selected.

Data Type	Collection Method	What are the subjects told about the intended use of their information?	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	All	All	Written
Family Relation (spouse, children, parents, grandparents, etc)	ALL	All	All	Written
Service Information	ALL	All	All	Written
Medical Information	ALL	All	All	Written
Criminal Record Information	ALL	Eligibility	All	Written
Guardian Information	ALL	All	All	Written
Education Information	ALL	Employment requirements	Written	Written
Benefit Information	ALL	All	All	Written
Other (Explain on Tab 8)				

Data Type	Storage Method	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran, VistA, Guardian	<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary
Family Relation (spouse, children, parents, grandparents, etc)	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran, VistA	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary
Service Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran, VistA	<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary
Medical Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran, VistA, Non-VA Provider	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary
Criminal Record Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran, FBI,	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary
Guardian Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary
Education Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary
Benefit Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary
Other (Explain on Tab 8)	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary

	(Please Select Yes/No)
Proximity and Timing: Is the privacy notice provided at the time of data collection?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	<input checked="" type="radio"/> Yes <input type="radio"/> No
routine use(s)	

(FY 2012) PIA: Data Sharing *Green Highlight = Must Answer Question		** Any connection external to VA requires an ISA/MOU per VA 6500. This section below must be consistent with your System Security Plan Interconnection Security Agreement section.			
Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VA Regional Counsel, VBA, Vet Center, CMOP, CPAC	<input checked="" type="radio"/> Yes <input type="radio"/> No	All	<input checked="" type="radio"/> Yes <input type="radio"/> No	Internal
Other Veteran Organization	Paralyzed Veterans of America	<input checked="" type="radio"/> Yes <input type="radio"/> No	Payments, Compensation, Healthcare	<input checked="" type="radio"/> Yes <input type="radio"/> No	VA Release of Information Form; Power of Attorney; CPRS Read-only
Other Federal Government Agency	None	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
State Government Agency	Cameron Veterans Home, Warrensburg Veterans Home, Missouri Department of Health and Senior Services	<input checked="" type="radio"/> Yes <input type="radio"/> No	Healthcare	<input checked="" type="radio"/> Yes <input type="radio"/> No	Other (Explain in Tab 8)
Local Government Agency	Kansas City Police Dept., Kansas City Health Dept.	<input type="radio"/> Yes <input checked="" type="radio"/> No	Other (Explain in Tab 8)	<input type="radio"/> Yes <input checked="" type="radio"/> No	Other (Explain in Tab 8)
Research Entity	Kansas University Medical Center, University of Missouri	<input checked="" type="radio"/> Yes <input type="radio"/> No	Healthcare	<input checked="" type="radio"/> Yes <input type="radio"/> No	VHA Handbook 1200.12
<input type="checkbox"/> Other Project/ System (Explain on Tab 8)					
(FY 2012) PIA: Access to Records					
Does the system gather information from another system?		<input checked="" type="radio"/> Yes <input type="radio"/> No			
Please enter the name of the system:		Health Eligibility Center (HEC), U.S. Postal Service, Internal Revenue Service			
(FY 2012) PIA: Secondary Use					
Will PII data be included with any secondary use request?		<input checked="" type="radio"/> Yes <input type="radio"/> No	<input type="checkbox"/> Mental Health	<input checked="" type="checkbox"/> HIV	<input type="checkbox"/> Drug/Alcohol Counseling
Check all that apply		<input type="checkbox"/> Sickle Cell	<input type="checkbox"/> Other (Explain on Tab 8)	<input checked="" type="checkbox"/> Research	

(FY 2012) PIA: Records Management		*Green Highlight = Must Answer Question	
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?			
<input type="radio"/> Yes (Explain on Tab 8) <input checked="" type="radio"/> No			
Is the data collected to only what is necessary to provide requested service?			
<input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8)			
Has the data provided been verified as complete?			
<input checked="" type="checkbox"/> Veteran Verified <input checked="" type="checkbox"/> Received From Database <input type="checkbox"/> Verification Unknown			
(FY 2012) PIA: Retention & Disposal			
What is the data retention period?		RCS 10-1 link for VHA: www.va.gov/vhapublications/rcs10/rcs10-1.pdf	
75 years		RCS VB-1, Part II Revised for VBA: www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/part2.pdf	
		National Archives and Records Administration: www.nara.gov	
Explain why the information is needed for the indicated retention period?			
To comply with Federal Law and facilitate the mission of the VA			
What are the procedures for eliminating data at the end of the retention period?			
VAMC Kansas City follows VA and VHA Records Management Handbooks and Directives including RCS 10-1 and GRS. Local Policy and			
Where are these procedures documented?			
VA Publications and VAMC Kansas City Records Management Policy and Procedures			
How are data retention procedures enforced?			
Designation of facility Records Manager, Service Line Liaisons, ongoing records management program to include file inventories,			
Has the retention schedule been approved by the National Archives and Records Administration (NARA)			
<input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8)			
(FY 2012) PIA: Children's Online Privacy Protection Act (COPPA)			
Will information be collected through the internet from children under age 13?			
<input type="radio"/> Yes (Explain on Tab 8) <input checked="" type="radio"/> No			

(FY 2012) PIA: Security *Green Highlight = Must Answer Question

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Is security monitoring conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Is security assessment conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Is adequate physical security in place to protect against unauthorized access?	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)

*Ensure PE 2, PE-3, PE-6, PE-7, PE-8 have been addressed appropriately for your categorization

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

<input checked="" type="checkbox"/> Biological Release	<input checked="" type="checkbox"/> Fire	<input checked="" type="checkbox"/> Lightning Strike	<input checked="" type="checkbox"/> Terrorism
<input checked="" type="checkbox"/> Blizzard	<input checked="" type="checkbox"/> Flood	<input checked="" type="checkbox"/> Malicious Code	<input checked="" type="checkbox"/> Thunderstorm
<input checked="" type="checkbox"/> Burglary/Break In	<input checked="" type="checkbox"/> Hacker, Cracker	<input checked="" type="checkbox"/> Password Privacy Negligence	<input checked="" type="checkbox"/> Tornado
<input type="checkbox"/> Civil Unrest	<input checked="" type="checkbox"/> Hail	<input checked="" type="checkbox"/> Personnel Unavailable	<input type="checkbox"/> Tsunami
<input checked="" type="checkbox"/> Component Failure	<input checked="" type="checkbox"/> HAZMAT Release/Spill	<input checked="" type="checkbox"/> Power Failure	<input checked="" type="checkbox"/> User Negligence
<input type="checkbox"/> Dam Failure	<input checked="" type="checkbox"/> Human Health Emergency	<input checked="" type="checkbox"/> Sabotage	<input checked="" type="checkbox"/> User Sabotage
<input type="checkbox"/> Dust/Debris	<input checked="" type="checkbox"/> Hurricane	<input checked="" type="checkbox"/> System Intrusion, Break-Ins	<input type="checkbox"/> Vibration
<input checked="" type="checkbox"/> Earthquake	<input checked="" type="checkbox"/> HVAC Failure	<input checked="" type="checkbox"/> System Misconfiguration	<input type="checkbox"/> Volcano
<input type="checkbox"/> Extreme Cold	<input checked="" type="checkbox"/> Indoor Humidity	<input checked="" type="checkbox"/> System Penetration	<input checked="" type="checkbox"/> Water Damage
<input type="checkbox"/> Extreme Heat	<input checked="" type="checkbox"/> Landslide	<input checked="" type="checkbox"/> System Tampering	<input checked="" type="checkbox"/> Winter Weather Hazards

*If any other risks identified, explain in Tab 8

Based upon the risks identified above, Explain what security controls are being used to mitigate these risks. (Check all that apply)

<input checked="" type="checkbox"/> Access Control	<input checked="" type="checkbox"/> Configuration Management	<input checked="" type="checkbox"/> Media Protection	<input checked="" type="checkbox"/> System and Services Acquisition
<input checked="" type="checkbox"/> Audit and Accountability	<input checked="" type="checkbox"/> Contingency Planning	<input checked="" type="checkbox"/> Personnel Security	<input checked="" type="checkbox"/> System and Communication Protection
<input checked="" type="checkbox"/> Awareness and Training	<input checked="" type="checkbox"/> Identification and Authentication	<input checked="" type="checkbox"/> Physical and Environmental Protection	<input checked="" type="checkbox"/> System and Information Integrity
<input checked="" type="checkbox"/> Security Assessment and Authorization	<input checked="" type="checkbox"/> Incident Response	<input checked="" type="checkbox"/> Risk Assessment	<input checked="" type="checkbox"/> Planning
			<input checked="" type="checkbox"/> Maintenance

Answer: (Other Controls) Explain on Tab 8

PIA: PIA Assessment

Based upon NIST 800-60, volume II; List the Information data types chosen as a basis for your FIPS 199 System Categorization.

Answer: D.14.4

<p>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)</p>	<input checked="" type="checkbox"/> 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. <input type="checkbox"/> The potential impact is moderate if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> The potential impact is low if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
<p>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)</p>	<input checked="" type="checkbox"/> 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. <input type="checkbox"/> The potential impact is moderate if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> The potential impact is low if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.
<p>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)</p>	<input checked="" type="checkbox"/> 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. <input type="checkbox"/> The potential impact is moderate if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> 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.

(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.

Tab 5

State Govt. Agencies: Vet homes have access to CPRS read-only and are authorize via a HIPAA Autorization. Missouri Department of Health and Senior Services does not have access to our system. Any information provided is authorized via a Standing Letter.

Local Govt. Agencies: Gunshot wound information is shared with the KC Police Dept. and is authorized via law and Standing Letter. Information regarding criminal investigations is also shared via Standing Letter. Information regarding certain medical conditions, including but not limited to TB, AIDS, STDs, etc is shared with the KC Health Department. This is authorized via law and Standing Letter.

(FY 2012) PIA: VISTA Minor Applications N-Z

Which of these are sub-components of your system?				
X	National Cemetery Association	X Pharmacy Data Management	Scanning Exam and Evaluation System	X VBECs
X	National Drug File	X Pharmacy National Database	X Scheduling	X VDEF
X	National Laboratory Test	X Pharmacy Prescription Practice	Security Suite Utility Pack	X Vendor - Document Storage Sys
	NDBI	X PICIS	X Sentillion	Veterans Canteen Web
X	Network Health Exchange	X Police & Security	X Shift Change Handoff Tool	Veterans Information Solution
X	NOAHLINK	X Problem List	ShoreTel	VHAHUNAPP1
	NOIS	X Progress Notes	Social Work	VHAHUNFPC1
	Nursing Service	X Prosthetics	Stellant	X VHS & RA Tracking System
	Occurrence Screen	X Purchase Order Management System	X Stentor	X Visit Tracking
X	Omnicell	X Pyxis	X Surgery	X VISTA RAD
X	Oncology	Q-Matic	Survey Generator	X VISTA RO
	Onicord (VLOG)	QMSI Prescription Processing	X Telecare Record Manager	X VistALink
	Optifill	Quality Assurance Integration	X Temp Trak	X VistALink Security
X	Order Entry/ Results Reporting	Quality Improvement Checklist	X Text Integration Utilities	X Visual Impairment Service Team ANRV
X	Outpatient Pharmacy	X QUASER	Tickler Database	Vitria BusinessWare
	P2000 ROBOT	X Radiology/ Nuclear Medicine	X Toolkit	VIXS
X	PACS database	RAFT	X TopCon	X Voluntary Timekeeping
	Patch Module	X RALS	TraceMaster	X Voluntary Timekeeping National
	Patient Data Exchange	X Record Tracking	Tracking Continuing Education	WEB HINQ
	Patient Feedback	X Registration	Traumatic Brain Injury	Whiteboard
	Patient Representative	X Release of Information - DSSI	Unwinder	X Women's Health
X	PCE Patient Care Encounter	X Remote Order/ Entry System	Utility Management Rollup	Workload and Overtime
	Personal Computer Generated Letters	X RPC Broker	Utilization Review	
	Pharmacy Benefits Mangement	Run Time Library	VA Conference Room Registration	
		X SAGG	X VA Fileman	
		X SAN	VAMedSafe	

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		*Green Highlight = Must Answer Question	
Facility Name:	Kansas City, MO		
Title:	Name:	Phone:	Email:
Privacy Officer:	Gayle Gregory	816-861-4700 x57101	gayle.gregory@va.gov
Digital Signature Block			
Information Security Officer:	David Collins	816-922-2038	david.collins4@va.gov
Digital Signature Block			
System Owner/Delegate:	George Parry	816-701-3048	george.parry@va.gov
Digital Signature Block			
Chief Information Officer:	Eddie Johnson	816-861-4700 x54295	eddie.johnson3@va.gov
Digital Signature Block			
R2 SMD Reviewer	Sandra Hedtke	701-237-2566	sandra.hedtke@va.gov
Digital Signature Block			
Date of Report:	2/2012		
OMB Unique Project Identifier	029-00-01-11-01-1180-00		
Project Name	REGION 2 > VHA > VISN 15 > Kansas City VAMC > Vista - VMS		
<p>The Signature Process:</p> <ul style="list-style-type: none"> • Complete the PIA form. • Name the PIA Excel FORM ["FY12-Region # - Facility Name - Facility # -Date(mmddyyyy).xls"] <ul style="list-style-type: none"> • Example: "FY12-Region3-Lexington VAMC-596-10302008.xls" • Submit the completed PIA Excel form to SMART Database. • Fix errors the reviewers sent back, rename the file and submit to SMART Database <ul style="list-style-type: none"> • If no errors, convert form into PDF with Nuance PDF Professional. • Name the PIA PDF form ["FY12-Region #-Facility Name- Facility # -Date(mmddyyyy).xls"] <ul style="list-style-type: none"> • Obtain digital signatures on the "Final Signatures tab" • Submit signed PIA PDF form to the SMART Database. 			