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://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 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 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

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:	Region 2>VHA>/VISN15>/Wichita VAMC /LAN
OMB Unique System / Application / Program Identifier (AKA: UPID #):	029-00-02-00-01-1120-00
Description of System / Application / Program:	General Support System, supporting mission-critical and other systems necessary to conduct day-to-day operations within VHA. Applications and devices within the LAN support numerous areas, including VistA, medical imaging, supply management, decision support, medical research, human resources, business operations, and education.

Facility Name: Robert J. Dole VAMC

Title:	Name:	Phone:	Email:
Privacy Officer:	Richard DiCaprio	316 688-6862	richard.dicaprio@va.gov
Information Security Officer:	Rolando Trevino	316 685-2221	rolando.trevino@va.gov
Chief Information Officer:	Sharon Williamson	316 634-3079	sharon.williamson@va.gov
Person Completing Document:	Richard DiCaprio	316 688-6862	richard.dicaprio@va.gov
Network Manager:	Wallace Harrell	316-634-3034	wallace.harrell@va.gov

Other Titles:	N/A
Other Titles:	N/A
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	08/2008
Date Approval To Operate Expires:	08/2011

What specific legal authorities authorize this program or system:	Title 38, United States Code, section 7301(a)
What is the expected number of individuals that will have their PII stored in this system:	1,000,000-9,999,999
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.	01/1995
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes
If No, please explain:	
Has a PIA been completed within the last three years?	Yes
Date of Report (MM/YYYY):	03/2010

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?
- ☐ 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?

☑ 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):	24VA19, 90VA194, 34VA12, 79VA19, 89VA19, 113VA112, 77VA10Q, 121VA19
2. Name of the System of Records:	Patient medical Records-VA, Call Detail Records-VA, Veteran,
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	N/A
Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?	Yes
Does the System of Records Notice require modification or updating?	No
	(Please Select Yes/No)
Is PII collected by paper methods?	Yes
Is PII collected by verbal methods?	Yes
Is PII collected by automated methods?	No
Is a Privacy notice provided?	Yes
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?	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)	Paper & Electronic	Privacy Notice	Verbally	Verbally
Family Relation (spouse, children, parents, grandparents, etc)	Paper & Electronic	Privacy Notice	Automated	Written
Service Information	Paper & Electronic	Privacy Notice	Verbally	Written
Medical Information	Paper & Electronic	Privacy Notice	Verbally	Written
Criminal Record Information	Electronic/File Transfer	Privacy Notice	Written	Written
Guardian Information	Paper & Electronic	Privacy Notice	Written	Written
Education Information	Electronic/File Transfer	Privacy Notice	Written	Written
Benefit Information	Electronic/File Transfer	Privacy Notice	Written	Written
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	
Service Information	Yes	Other Federal Agency (Identify)	Mandatory	
Medical Information	Yes	Veteran	Voluntary	
Criminal Record Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Guardian Information	Yes	Veteran	Voluntary	
Education Information	Yes	Veteran	Voluntary	
Benefit Information	Yes	Veteran	Mandatory	
Other (Explain)				
Other (Explain)				
Other (Explain)				

(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	Veterans Benefits Administration (VBA)	Yes	payment, treatement and healthcare operations	Both PII & PHI	Ref. 45 CFR 164.512; 5USC 552
Other Veteran Organization	Vet Center	Yes	payment, treatement and healthcare operations	Both PII & PHI	Ref. 45 CFR 164.512; 5USC 552
Other Federal Government Agency	No				
State Government Agency	Kansas Veterans Home, Winfield	Yes	payment, treatement and healthcare operations	Both PII & PHI	CPRS Read-Only Access VHA Directive, VA Form 10-5345
Local Government Agency	No				
Research Entity	Kansas University Medical Center	Yes	Patient Health Records for Research purposes	Both PII & PHI	VHA Handbook 1200.12
Other Project / System	QuadraMed	Yes	Data is not shared	Both PII & PHI	National BAA
Other Project / System	N/A				
Other Project / System	N/A				

(FY 2010) PIA: Access to Records

Does the system gather information from another system?	No
Please enter the name of the system:	Region 2>VHA>/VISN15>/Wichita VAMC /LAN
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:	☐ 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?	Yes
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:	VA Handbook and Directives 6500, VHA Handbooks 1605.1 and 1605.3 Minimum Necessary per VHA Handbook 1605.2

(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:

Explain how collected data are limited to required elements:
PI is collected to be stored in The RIS system. This system is not located on site. IT only maintains systems we do not dictate or controll the collection of data.

How is data checked for completeness?
Answer: Each Service Line conducts monitors and audits per regulatory requirements (i.e. IG, JCAHO, etc.).

What steps or procedures are taken to ensure the data remains current and not out of date?
Answer: Patient information is updated and/or verified at pt. visits, (i.e. Means Test,

How is new data verified for relevance, authenticity and accuracy?
Answer: Local Medical Center Policies & Controls

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

Answer:

(FY 2010) PIA: Retention & Disposal

What is the data retention period?
Answer: Destroy/delete when 3 years old

Explain why the information is needed for the indicated retention period?
Answer: 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 Wichita follows VA and VHA Records Management Handbooks and Directives including RCS 10-1, RCS005-1, and GRS. Local Policy and desgination of responsibilities in place

Where are these procedures documented?
Answer: VA Publications and VAMC Wichita Records Management Policy and Procedures

How are data retention procedures enforced?
Answer: VA Publications

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 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: Security controls have been defined, implemented and monitored in accordance with VA Directive / Handbook 6500.	

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

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

Answer: (Other Risks)

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

- [x] Risk Management
- [x] Access Control
- [x] Awareness and Training
- [x] Contingency Planning
- [x] Physical and Environmental Protection
- [x] Personnel Security
- [x] Certification and Accreditation Security Assessments
- [x] Audit and Accountability
- [x] Configuration Management
- [x] Identification and Authentication
- [x] Incident Response
- [x] Media Protection

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. Sensitivity of data was reviewed with no required changes

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 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)

- [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.

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: