Welcome to the PIA for FY09!

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 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.

(FY 09) PIA: System Identification

Program or System Name:	Region 3>VHA>VISN11>NIHCS (610)>LAN
OMB Unique System / Application / Program Identifier (AKA: UPID #):	**029-00-02-00-01-1120-00**
Description of System / Application / Program:	Each VA medical center uses the Local Area Network (LAN) as a General Support System, supporting mission-critical and other systems necessary to conduct day-to-day operations within the Veterans Health Administration. Applications and devices within the LAN support numerous areas, including medical imaging, supply management, decision support, medical research, and education.
Facility Name:	VA Northern Indiana Health Care System

Title:	Name:	Phone:	Email:
Privacy Officer:	Jane Sowers	260-421-1058	jane.sowers@va.gov

Information Security Officer:	Scott A. Dubois	765-677-3171	scott.dubois@va.gov
Chief Information Officer:	David C. Troyer	765-677-6100	david.troyer@va.gov
Person Completing Document:	Scott A. Dubois	765-677-3171	scott.dubois@va.gov
Other Titles:			

Other Titles:	
Other Titles:	
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:	approximately 1,000,000
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.	09/1996
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes
If No, please explain:	

Date of Report (MM/YYYY):	04/2009

If answers 'Yes' to one or more of the following, please check the appropriate box, continue to the next tab, and complete the remaining questions on this form. If none have been checked then skip to Signatures tab, obtain the appropriate signatures, and submit this document.

- [ ] Has a PIA NOT been completed within the last three years?
- [x] 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?

(FY 09) 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):	79VA19, 24VA19
2. Name of the System of Records:	LAN
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	http://vaww.vhaco.va.gov/privacy/Systemofecords.htm
Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?	Yes
Does the System of Records Notice require modification or updating?	Yes
	(Please Select Yes/No)
Is PII collected by paper methods?	Yes
Is PII collected by verbal methods?	Yes
Is PII collected by automated methods?	Yes
Is a Privacy notice provided?	Yes
Proximity and Timing: Is the privacy notice provided at the time of data collection?	Yes
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	Yes
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	Yes
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	Yes

(FY 09) 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 messaged conveyed to them?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Verbal	The most common data types that are captured and accessed on a regular basis by authorized individuals are first and last name, middle initial, DOB, SSN, and address. This patient information falls into two classes: administrative and clinical. Clinical information is used to diagnose, prescribe treatment and follow clinically the patient through his/her health care encounters. Administrative data is used to identify the veteran (SSN), correspond to/from (name and address), and determine eligibility (patient administrative info + SSA and IRS data).	Verbally
Family Relation (spouse, children, parents, grandparents, etc)	Paper	Dependent Data is utilized to determine eligibility for VA benefits. In addition, NOK and emergency contact information is often a	Written

Service Information	Electronic/File Transfer	Military Service Information (Branch of service, discharge date, discharge type, service connection rating, medical conditions related to military service, etc). This information is collected to assess eligibility for VA healthcare benefits, type of healthcare needed.	Verbally
Medical Information	Verbal	VistA-Legacy applications and meet a wide range of health care data needs. The VistA-Legacy system operates in medical centers, ambulatory and community-based clinics, nursing homes and domiciliary, and thus collects a wide range of personal medical information for clinical diagnosis, treatment, patient evaluation, and patient care. Common types of personal medical information would include lab test results, prescriptions, allergies, medical diagnoses, vital signs, etc. The information is used to treat and care for the veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of the veteran.	Verbally

Criminal Record Information	Electronic/File Transfer	Specific information is not input into the VistA system but the fugitive felon program includes a flag on the patient file identifying the need to contact the VA police.	Verbally
Guardian Information	Verbal	Guardian information is often flagged in the medical record to ensure the timely and appropriate notification during healthcare decision making from provider/patient/guardian.	Written
Education Information		N/A	
Benefit Information	Electronic/File Transfer	VIS, HINQ, VERA, KLF, used to verify service dates, eligibility, SSN, etc.	Written
Other (Explain)	Paper	Next-of-kin information and emergency contact information, such as name and telephone number, is collected from the veteran to use to contact other individuals in case of an emergency. In addition insurance and employment information is available on the veteran for use in billing for care. Religious information is collected to provide for spiritual needs if requested by the veteran.	Written

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?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Mandatory
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory
Medical Information	Yes	Veteran	Mandatory
Criminal Record Information	Yes	State Agency (Identify)	Mandatory
Guardian Information	Yes	Veteran	Mandatory
Education Information	Yes	Veteran	Mandatory
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory
Other (Explain) Other (Explain) Other (Explain)			

How is a privacy notice provided?

Verbally

Written

Written

Written

Written

Written

Written

Written

Additional Comments
VBA
Fugitive Felon
VBA

(FY 09) 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	VBA	No	treatment and demographic for benefits determination	Both PII & PHI	
Other Veteran Organization	Office of Regional Counsel	No	Tort Claims, legal processes	Both PII & PHI	
Other Federal Government Agency	Congressional Offices	No	Appointment dates, treatment, medical documentation, bills, co-pays	Both PII & PHI	
State Government Agency	CDC	No	HIV Results	Both PII & PHI	
Local Government Agency	N/A				
Research Entity		No		Both PII & PHI	
Other Project / System					
Other Project / System					
Other Project / System					

(FY09) PIA: Access to Records

Does the system gather information from another system?	Yes
Please enter the name of the system:	Vista

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

(FY09) 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:	

(FY 09) PIA: Program Level Questions

Does this PIA 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: By the Vista system, staff and the data validation comittee

How is data checked for completeness?

Answer: By the Vista system, staff and the data validation comittee

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

Answer: Policies and PI reviews

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

Answer: Staff and PI reviews

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

Answer:

(FY 09) PIA: Retention & Disposal

What is the data retention period?

Answer: 75 years after the last episode of care.

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

Answer: Clinical information is retained in accordance with VA Records Control Schedule 10-1.

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

Answer: Electronic Final Version of Patient Medical Record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records Control Schedule 10-1, Item XLIII, 2.b. (Page 190).

Where are these procedures documented?

Answer: Record Control Schedule 10-1

How are data retention procedures enforced?
Answer: Program officials are responsible for creating, maintaining. protecting, and disposing of records in their program area in accordance with NARA regulations and VA policy. All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures.

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 09) 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 09) 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:	

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

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

- [x] Personnel Security
- [x] 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: Reviewed data collection methods.

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:

FY 09: 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 09) PIA: Final Signatures

Facility Name: VA Northern Indiana Health Care System

Title:	Name:	Phone:	Email:
Privacy Officer:	Jane Sowers	260-421-1058	jane.sowers@va.gov
Digital Signature Block	JANE SOWERS	Digitally signed by JANE SOWERS DN: o=Department of Veterans Affairs, ou=Dept. of Veterans Affairs, Internal Staff, ou=www.verisign.com/repository/CPS Incorp. by Ref.,LIAB.LTD(c)96, cn=JANE SOWERS, email=jane.sowers@va.gov Date: 2009.07.29 11:40:52 -04'00'	
Information Security Officer:	Scott A. Dubois	765-677-3171	scott.dubois@va.gov
Digital Signature Block	SCOTT DUBOIS	Digitally signed by SCOTT DUBOIS DN: o=Department of Veterans Affairs, ou=Dept. of Veterans Affairs, Internal Staff, ou=www.verisign.com/repository/CPS Incorp. by Ref.,LIAB.LTD(c)96, cn=SCOTT DUBOIS, email=scott.dubois@va.gov Date: 2009.07.28 14:23:59 -04'00'	
Chief Information Officer:	David C. Troyer	765-677-6100	david.troyer@va.gov
Digital Signature Block	DAVID TROYER	Digitally signed by DAVID TROYER DN: cn=DAVID TROYER, o=Department of Veterans Affairs, ou=Dept. of Veterans Affairs, Internal Staff, email=david.troyer@va.gov Date: 2009.07.29 11:21:47 -04'00'	
Person Completing Document:	Scott A. Dubois	765-677-3171	scott.dubois@va.gov
Digital Signature Block	SCOTT DUBOIS	Digitally signed by SCOTT DUBOIS DN: o=Department of Veterans Affairs, ou=Dept. of Veterans Affairs, Internal Staff, ou=www.verisign.com/repository/CPS Incorp. by Ref.,LIAB.LTD(c)96, cn=SCOTT DUBOIS, email=scott.dubois@va.gov Date: 2009.07.28 14:24:25 -04'00'	
System / Application / Program Manager:	0	0	0
Digital Signature Block			

Date of Report:	4/18/2009
OMB Unique Project Identifier	029-00-02-00-01-1120-00
Project Name	Region 3>VHA>VISN11>NIHCS (610)>LAN