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 3 > VHA > VISN 10 > Cleveland VAMC > VistA
OMB Unique System / Application / Program Identifier (AKA: UPID #):	029-00-01-11-01-1180-00
Description of System / Application / Program:	The Cleveland VAMC VistA system is a Major Application owned by VA that has been determined to have a security categorization of HIGH in accordance with FIPS Publication 199.

Facility Name:	Louis Stokes Cleveland VAMC

Title:	Name:	Phone:
Privacy Officer:	Joseph Picklo	216-791-3800 ext 5539
Information Security Officer:	Larry Campbell	440-526-3030 ext 6625
Chief Information Officer:	Steve Gaj	440-526-3030 ext 7755
Person Completing Document:	Larry Campbell	440-526-3030 ext 6625
Other Titles:		
Other Titles:		
Other Titles:		

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	07/2008
Date Approval To Operate Expires:	08/2011
What specific legal authorities authorize this program or system:	Record System 79VA19/Title 38, United States Code, section 7301(a)
What is the expected number of individuals that will have their PII stored in this system:	500,000

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.	23.00
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 fo

- ☐ Have any changes been made to the system since the last PIA?
- ☐ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- ☑ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- ☑ Does this system/application/program collect, store or disseminate PII/PHI data?
- ☑ Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please skip to TAB 12. (See Comment for Definit

Email:
joseph.picklo@va.gov larry.campbell@va.gov steven.gaj@va.gov larry.campbell@va.gov

form

s, or others performing work

ntifier, symbol, or othe

ıition of PI

(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):	79VA19	
2. Name of the System of Records:	Veterans Health Information System and Technology Architechture (VistA)-VA	
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	2003 Privacy Act Compilation published in Federal Register. http://vaww.vhaco.va.gov/privacy/systemofrecords.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?	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?	Yes	
Is a Privacy notice provided?	Yes	
Proximity and Timing: Is the privacy notice provided at the time of data collection?	Yes	
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	Yes	
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	Yes	
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	Yes	

(FY 2010) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Paper & Electronic	Benefits, Healthcare	Verbal & Written	Verbal & Written
Family Relation (spouse, children, parents, grandparents, etc)	Paper & Electronic	Benefits, Healthcare	Verbal & Written	Verbal & Written
Service Information	Paper & Electronic	Benefits, Healthcare	Verbal & Written	Verbal & Written
Medical Information	Paper & Electronic	Benefits, Healthcare	Verbal & Written	Verbal & Written
Criminal Record Information	VA File Database	Benefits, Healthcare	Verbal & Written	Verbal & Written
Guardian Information	Paper & Electronic	Benefits, Healthcare	Verbal & Written	Verbal & Written
Education Information	Paper & Electronic	Benefits, Healthcare	Verbal & Written	Verbal & Written
Benefit Information	Paper & Electronic	Benefits, Healthcare	Verbal & Written	Verbal & 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	Veteran	Mandatory	On-Form
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Mandatory	On-Form
Service Information	Yes	Veteran	Mandatory	On-Form
Medical Information	Yes	Veteran	Mandatory	On-Form
Criminal Record Information	Yes	VA Files / Databases (Identify file)	Mandatory	On-Form
Guardian Information	Yes	Veteran	Mandatory	On-Form
Education Information	Yes	Veteran	Mandatory	On-Form
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	On-Form
Other (Explain): Fugitive Felon Program				
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	VSO, VBA, AAC, VACO, CMOP, eCME, DDC, NPPD	Yes	limited patient information used for eligibility benefits.	Both PII & PHI	DSS ROI, VHA HB1605.1
Other Veteran Organization		No			
Other Federal Government Agency	IRS, DoD, SSA,	No	Benefits, Health info, Income matching	Both PII & PHI	DSS ROI, sharing agreements
State Government Agency		No			
Local Government Agency		No	Public Health, Infectious Disease Information	Both PII & PHI	Florida Department of Health Procedures, DSS ROI
Research Entity	NONE	No			
Other Project / System	Private Insurance Companies, Medicare, Tricare	No	Insurance/payment Information	Both PII & PHI	ROI, BAA
Other Project / System	None	No			
Other Project / System	None	No			

(FY 2010) PIA: Access to Records

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

(FY 2010) PIA: Secondary Use

Will PII data be included with any secondary use request?	No				
if yes, please check all that apply:	☐ Drug/Alcohol Counseling ☐ Mental Health ☐ HIV ☐ Research ☐ Sickle Cell ☐ Other (Please Explain)				
Describe process for authorizing access to this data.					
Answer:					

(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: Answer: Data is collected electronically based on the automation of VA Forms and clinical procedures which are configured to request only the information required. Approved templates (Medical record Committee) and SOPs are used for medical information collecting; scripts are used by staff. Forms are also standardized nationally.		
How is data checked for completeness? Answer: Data is reviewed by staff and compared to paper forms. Various audits such as medical record audit, compliance audits in MCCR, etc, ensure completeness. Electronic collection of data (administration and clinical) can be controlled through prompts, required "indicators", instructions on forms and training of staff. Electronic clinical templates use similar techniques as well as character-limited fields, type of response fields used in the template (yes/no, checkbox, text response), field size and required indicators (*). National and local policies and procedures also "limit", define what information is collected. Licenses and certifications of various clinical staff define "scopes of practice" and limit information needed for care and treatment from specific treating individuals. Policies and procedures work the same way for administrative data collected. The United States Code of Federal Regulations, Privacy Act of 1974, the Freedom of Information Act and the Health Insurance Portability and Accountability Act are federal regulations that govern VHA healthcare facilities. Standards for medical documentation, Joint Commission standards and other regulatory agencies also dictate information to be collected.		
What steps or procedures are taken to ensure the data remains current and not out of date? Answer: VHA staff checks for completeness, accuracy, and currency by reviewing the forms. The patient		
How is new data verified for relevance, authenticity and accuracy? Answer: Much of the same information provided in data completeness question above applies to this question. Signature verification is often performed by comparison to other signed documents. Some procedures may require notarized documents (ROI and copies of records in some instances). Relevance is determined through review by knowledgeable staff for both administrative and clinical information, data fields on forms and regulations. HINQs are another source for verifying information.		
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: 75 years		
Explain why the information is needed for the indicated retention period?		

Answer: Retention periods for data vary according to the type of records. Data owners are responsible for ensuring they follow the record retention periods outlined in RCS 10-1.		
What are the procedures for eliminating data at the end of the retention period?		
Answer: For VHA projects, VHA Handbook 1907.1 (Section 6j) and VHA Records Control Schedule 10-1 provide more general guidance.		
Where are these procedures documented?		
Answer: For VHA projects, VHA Handbook 1907.1 (Section 6j) and VHA Records Control Schedule 10-1 provide more general guidance.		
How are data retention procedures enforced?		
Answer: For VHA projects, VHA Handbook 1907.1 (Section 6j) and VHA Records Control Schedule 10-1 provide more general guidance.		
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: Privacy Act, 5 U.S.C. 552A(E)(4)							

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

- [x] Air Conditioning Failure
- [x] Chemical/Biological Contamination
- [ ] Blackmail
- [ ] Bomb Threats
- [ ] Cold/Frost/Snow
- [ ] Communications Loss
- [x] Computer Intrusion
- [x] Data Destruction
- [x] Data Disclosure
- [x] Data Integrity Loss
- [x] Denial of Service Attacks
- [ ] Earthquakes
- [x] Eavesdropping/Interception
- [ ] Fire (False Alarm, Major, and Minor)
- [ ] Flooding/Water Damage
- [x] Hardware Failure
- [x] Malicious Code
- [x] Computer Misuse
- [x] Power Loss
- [ ] 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

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.

Answer: Keeping existing procedures

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☐ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
	☑ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☑ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
	☐ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? **(Choose One)**	☐ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☑ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
	☐ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
The controls are being considered for the project based on the selections from the previous assessments? The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.	
Please add additional controls:	