

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://vawww.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 an individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirectly identify 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: Local Area Network (LAN) for Marion, IL VAMC

OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-02-00-01-1120-00

The LAN system is comprised of network devices, workstations, servers, printers, and other devices which support communications, to include routers, hubs, switches, firewalls, etc. The LAN includes magnetic tape drives, disk drives, and uninterruptible power supplies (UPS). Access to the system is via work stations operating on Windows-family Operating Systems (O/S), Windows XP, and thin-client terminals located throughout the medical center complex. Microsoft Windows client workstations connect over a Windows network and may use terminal emulation software and the Remote Procedure Call (RPC) Broker to connect to other systems such as Vista. There is access from the Intranet to both the VA's wide area net work (WAN) and to the Internet via the VA Internet gateways. The LAN provides connectivity for one Medical Center, three annexes, 8 CBOCs, and one Vet Center.

Facility Name: VA Medical Center, Marion, IL (657A5)

Title: Name: Phone:

Privacy Officer:	Deanna Duncan	618-997-5311,)
Information Security Officer:	Terry Taylor	618-997-5311,)
Chief Information Officer:	Clint Bishop	618-997-5311,)
Person Completing Document:	Deanna Duncan	618-997-5311,)
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: Privacy Act of 1974; Federal Information Security Management Act of 2002; OMB Circular A-130; Computer Security Act of 1987; Freedom of Information Act; Health Insurance Portability and Accountability Act; Title 38, USC Section 7301(a)

What is the expected number of individuals that will have their PII stored in this system: 60,000 (estimate)

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. 21 years in operation

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):

02/2010

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on th

- Have any changes been made to the system since the last PIA? Added components, including annexes and CBOCs.
- Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA? No
- Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data? No
- Does this system/application/program collect, store or disseminate PII/PHI data? Yes
- Does this system/application/program collect, store or disseminate the SSN? Yes

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

Email: [REDACTED]

Deanna.Duncan@va.gov

Terry.Taylor@va.gov

Clint.Bishop@va.gov

Deanna.Duncan@va.gov



his form

g annexes

tors, or others performing work for

identifier, symbol, or other PII data

definition 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:

- A. 90VA194
- B. 89VA19
- C. 113VA112
- D. 77VA10Q
- E. 121VA19
- F. 24VA19

1. All System of Record Identifier(s) (number):

- A. Call Detail Records
- B. Income Verification Records
- C. Telephone Service for Clinical Care Records
- D. Health Care Provider C&P Records
- E. National Patient Databases
- F. Patient Medical Records

2. Name of the System of Records:

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

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?	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)	Verbal	Healthcare	Verbally	Verbal & Written
Family Relation (spouse, children, parents, grandparents, etc)	Verbal	Healthcare	Verbally	Verbal & Written
Service Information	Paper & Electronic	Healthcare, employment	Verbal & Automatic	Verbal & Written
Medical Information	ALL	Healthcare	All	All
Criminal Record Information	VA File Database	Employment	Written	Written
Guardian Information	Paper	Healthcare	Verbal & Written	Verbal & Written
Education Information	ALL	Employment requirement	All	All
Benefit Information	ALL	Healthcare, benefits	All	All
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 (Explain)	Mandatory	Verified via DD2-14. Information used for eligibility purposes and veteran preference for employment.

Medical Information

Yes

VA Files / Databases (Identify file)

Mandatory

Privacy and security notice is shown at VistA login.

Criminal Record Information

Yes

Other Federal Agency (Identify)

Mandatory

Office of Personnel Management. Information is used for employee processing in compliance with OPM regulations

Guardian Information

Yes

Veteran

Voluntary

Education Information

Yes

VA Files / Databases (Identify file)

Mandatory

Employee training and education is tracked via LMS and TEMPO.

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	VA Regional Counsel	Yes	CPRS medical records; healthcare operations and legal services	Both PII & PHI	Ref. 45 CFR 164.512; 38 USC 7332[b]; 38 USC 5701[b]
Other Veteran Organization	Vet Center	Yes	Access is limited to data stored on server; treatment and healthcare operations	Both PII & PHI	Ref. 45 CFR 164.512; 38 USC 7332[b]; 38 USC 5701[b]
Other Federal Government Agency	N/A				
State Government Agency	N/A				
Local Government Agency	N/A				
Research Entity	N/A				
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2010) PIA: Access to Records

Does the system gather information from another system? Yes
 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

Drug/Alcohol Counseling Mental Health HIV

if yes, please check all that apply:

Research Sickle Cell Other (Please Explain)

Describe process for authorizing access
to this data.

Answer: N/A

(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: Employee education and as outlined in local and national policies.

How is data checked for completeness?

Answer: Each Service Line conducts monitors and audits per regulatory requirements (i.e. IG, JCHO, etc.).

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

Answer: Each Service Line conducts monitors and audits per regulatory requirements (i.e. IG, JCHO, etc.).

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

Answer: Internal 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: Data is retained in accordance with RCS-10. Length of retention varies by type of information being stored.

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

Answer: Healthcare.

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

Answer: Hard drives and tapes are sanitized by degaussing and shredding. Memory cards are sanitized by shredding.

Where are these procedures documented?

Answer: Sanitization procedures are documented in Medical Center Memorandum 085 Information Security and IRM SOP.

How are data retention procedures enforced?

Answer: The Records Management Officer is responsible for oversight of information retention.

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: A review and certification of security controls within the LAN is completed every 3 years and the system's operation is formally approved at that time in accordance with the requirements of OMB Circular A-130, Appendix III. The Marion, IL VAMC has implemented NIST 800-53's baseline of minimum security controls for the LAN in accordance with the Federal Information Security Management Act of 2002 (Title III of e-Gov). Security of the LAN is managed through the VA FISMA/SMART Reporting Tool to ensure that security is addressed throughout the life cycle of the system. The FISMA/SMART Reporting Tool tracks vulnerability remediation efforts through the Plan of Action and Milestones (POA&Ms), and is a document repository for C&A efforts.

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)

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

The potential impact is **high** if the loss of availability could be expected to have a severe 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.

Answer: (Other Controls)

PIA: PIA Assessment

The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

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.

Answer: **Increased security controls.**

The potential impact is **moderate** if the loss of availability could be expected to have a

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 **critical** if the loss of availability could be expected to have a catastrophic 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 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.

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 **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 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: