

Information Security



Information Security for Research

Thursday October 14th 2010

Information Security Officers (ISO)

- Terry Peters
- (352)376-1611 x4114



- Patrick Cheek
- (352)376-1611 x4492





Overview

- Protocol Approval
- Sensitive Information
- Authority to Transport
- Electronic Data Storage
- Paper Data
- Storing VA Research Data at UF
- Data Transfer Agreements
- Confidentially
- Passwords
- Laptops
- Sponsor Equipment
- Backups
- PKI
- Incidents
- Media Disposal
- Other Information



Protocol ISO Approval

- Key items to be identified in your protocol.
 - Who is the sponsor?
 - Will sensitive data be transferred to the sponsor?
 - How are you transferring the data?
 - Will data be transported outside the protected environment?
 - Will any sensitive data be stored outside the protected environment?
 - Where will the electronic data be stored? Be specific.
 - Where will any paper data be stored? Be specific
 - Is there any sponsor provided computers, laptops, thumb drives?
 - Is the protocol approved at another VA facility and will data be transferred?



Sensitive Information

- **Sensitive Information:** VA sensitive information is all Department data, on any
- storage media or in any form or format, which requires protection due to the risk of harm
- that could result from inadvertent or deliberate disclosure, alteration, or destruction of
- the information. The term includes information whose improper use or disclosure could
- adversely affect the ability of an agency to accomplish its mission; proprietary
- information; records about individuals requiring protection under various confidentiality
- provisions such as the Privacy Act and the HIPAA Privacy Rule; and information that
- can be withheld under the Freedom of Information Act. Examples of VA sensitive
- information include the following: individually-identifiable medical, benefits, and
- personnel information; financial; budgetary; research; quality assurance; confidential
- commercial; critical infrastructure; investigation, and law enforcement information;
- information that is confidential and privileged in litigation such as that which is protected
- by the deliberative process privilege, attorney work-product privilege, or the attorney-client
- privilege; and other information which, if released, could result in violation of law
- or harm or unfairness to any individual or group, or could adversely affect the national
- interest or the conduct of federal programs.



Authority to Transport

- Required when removing **sensitive** data from the VA Protected Environment.
- Examples of outside the Protected Environment: Transporting to/from:
 - RORC to Malcom Randall
 - Malcom Randall to UF
 - Malcom Randall to Lake City



Authority to Transport

➤ Where do I get the form letter?

- ISO SharePoint Site under “Shared Documents” “Forms”.

<http://vaww.visn08.r03.portal.va.gov/northflorida/directorsoffice/infosecurity/default.aspx>

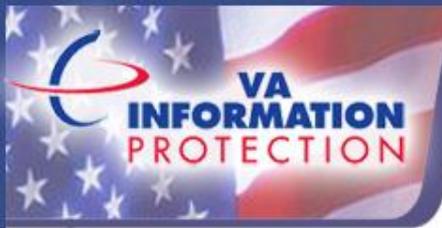


Authority to Transport

You must have a completed form signed by your supervisor, Service Chief, CIO, Director and ISO before you can transport.

Recommend you complete the form while your protocol is going through the approval process.





Electronic Data Storage

- Store your data in a secure folder on the VA network. The folder should only be accessible by investigators assigned to your study.
- Backup data stored on PCs and Thumb Drives daily to your secure folder on the VA network.

Paper Data

- Store in locked cabinets/containers inside the protected environment.
- Only investigators approved for your study should have access to the cabinets/containers.



Storing VA Research Data at UF

- Not authorized
- Why? VA electronic data must be stored on systems that are Federal Information Security Act (FISMA) compliant. UF computer system is not FISMA compliant.



Data Transfer/Data Use Agreements

- VHA Handbook 1200.12
- Use Appendix C to determine if a DTA/DUA is required for your study.
- If required submit

http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1851

Maintaining Confidentiality

*It is your responsibility

- Lock your computer
- automatic log off
- Ctrl + Alt + Delete

➤ Printing PII

- take it from the printer right away
- keep it stored in a secure place.

➤ Only access information you need to do your job.

➤ Never discuss a Veterans personal information in public



Passwords

- Must be changed every 90 days
- Have at least 8 characters
- Use at least 3 of the following
 - Upper-case letters (ABC...)
 - Lower-case letters (...xyz)
 - Special characters (#, &, *, or @)
 - Numbers (0123456789)



The screenshot shows the 'Change Password' dialog box in Windows XP. The title bar is blue and contains the text 'Change Password'. Below the title bar is the Microsoft logo and the text 'Microsoft Windows xp Professional'. The dialog box has a light beige background. It contains five input fields: 'User name:', 'Log on to:', 'Old Password:', 'New Password:', and 'Confirm New Password:'. The 'Old Password:', 'New Password:', and 'Confirm New Password:' fields are filled with black dots. At the bottom right, there are two buttons: 'OK' and 'Cancel'.



Strong Password Rules

➤ Do Not Use:

- words found in the dictionary
- personal references (name, birthday, address)
- automatic password-saving features

➤ Never let anyone stand near you while you type your password

➤ Keep it safe under lock and key

**Not under your keyboard or mouse!!



Laptops

- Must be purchased and authorized by IRM.
- Must be encrypted using FIPS 140-2 encryption.
- How do I know its Encrypted?
Contact IRM at 374-6093
- Returned every 90 days to IRM for checkup and updates.
- My laptop does not have a VA inventory label with an EE number? Your laptop may not be encrypted, contact IRM.



Thumb Drives

- Must request one in writing from IRM
- Request form is on the ISO SharePoint site
- Don't store PHI/PII on them unless you have to, and ensure it is encrypted



Sponsor Provided Equipment

➤ Laptops

- Must be approved by the ISO and CIO.
- Must be encrypted by IRM with a FIPS 140-2 approved encryption.
- Must be assigned an EE number by A&MMS.
- Hard drive must be removed and turned-in to IRM **before** the laptop is returned to sponsor.

➤ Thumb Drives

- Not approved for use. Only VA approved FIPS 140-2 encrypted thumb drives issued by IRM can be used.

Backing up Data

- Backing up important data
 - All VA data is backed up daily
 - Back up your data on a periodic basis
- Save information on a network drive such as your **Homedrive**
 - This will ensure your data is backed up in case of computer failure or an office relocation
 - Can log on to any computer with your data



PKI

➤ Using Public Key Infrastructure (PKI) to encrypt a message

- Validating authenticity
- Maintaining confidentiality
- Protection from alteration.



➤ REMEMBER: If you send Personally Identifiable Information (PII) in Outlook about a veteran or VA employee, it **must be encrypted!!**

Incident Identification and Reporting Computer Related Incidents

➤ Several Examples of Security Incidents include:

- A virus
- A lost or stolen computer
- Missing or compromised files
- Unauthorized sharing of sensitive information
- Unauthorized access of Government IT systems



➤ All information security incidents should be reported to your Supervisor, PO and ISO within 59 minutes!

Incident Identification and Reporting Computer Related Incidents

- If you think a security incident has occurred:
 - Gather information about what happened:
 - Date, time, location
 - Indicate the media that was compromised laptop, desktop, thumb drive, etc.
 - If a laptop or thumb drive was the data encrypted?
 - Was paper data involved?
 - How many veterans are affected?
 - What PHI/PII did the data contain? Name, DOB, SSAN, medical record, etc.



Media Disposal

- Clicking on the Delete button does NOT delete a file permanently from your computer.
 - Software can restore all deleted files
 - This is why hard drives are removed and destroyed from all PCs prior to leaving the VA



Media Disposal

- Contact your ISO or IT staff if you have any media that needs to be destroyed.

- To prevent accidental exposure of PII the VA has strict guidelines in place to ensure the proper sanitization and disposal of media containing VA sensitive information.
 - Hard Drives
 - CD-ROMs
 - Flash Drives
 - Optical Drives
 - Sensitive Documents





Other Information

- VPN from Malcom Randall to Shands
- VPN from Shands to Malcom Randall
- Storing VA Research Data at the Shands Data Center



Any Questions?

Terry Peters

(352)376-1611 x4114

Patrick Cheek

(352)376-1611 x4492

Trailer 9