Washington
WASHINGTON · UNIVERSITY · IN · ST · LOUIS
School of Medicine
Department of Radiation Oncology

HIPAA Security Procedure #17

Transmission Security Procedure

Last Revised: 3/15/2006	*Approved: -*

Scope:

This procedure prescribes security measures to be taken during transmission of EPHI by file transfer or use of email or messaging systems. WU networks do not physically restrict the transmission of EPHI out of the networks. Additional measures must be taken by the user to protect the security and privacy of EPHI.

Terms:

WUSTL	Washington University public network
WUCON	Washington University Clinical Operations private network
CARENET	BJC private network

Principles/Requirements:

a) Minimum Necessary:	Always transmit the minimum amount of EPHI necessary. (See HIPAA Privacy Policy #11- Minimum Necessary Request, Use or Disclosure of Protected Health Information.)
b) Authentication:	When transmitting EPHI electronically, Workforce members must take reasonable precautions to ensure that the receiving party is who they claim to be and has a legitimate need for the EPHI requested. Some encryption mechanisms may have their own method of authentication.
c) Within Private Network	RO/WUCON-WUCON, CARENET-CARENET transfers require no added security measures
d) Encryption level	All encryptions mechanisms described in these procedures will support a minimum of 128-bit encryption.
e) Transmit to CARENET	All file transfers to CARENET must authenticate to and pass through WUCON.

Security Measures (common examples):

a) Encryption during transmission
   1) Virtual Private Network (VPN)
   2) Secure Shell (SSH)
   3) Secure File Transfer Protocol (SFTP)
   3) CITRIX

b) Encryption of message or data file:
   1) Encrypted ZIP file plus password-protect (WinZip is one such product)
   2) S/MIME Encryption or Public Key/Private Key Encryption (planned)

c) Password protection of data file

1) File Transfer of EPHI Procedure: When performing file transfer of data containing PHI, use the following guidelines to determine the security measures necessary.

FROM	TO	USE
RO / WUCON	Outside these domains	Encrypt a) or b)
RO / WUCON	Unsecured WUSTL	Encrypt a) or b) OR password protect c)
RO / WUCON	CARENET	None necessary

2) Email or Messaging Systems (transmitting EPHI) Procedure:
(See also: **RO HIPAA Privacy Procedure 17-7, Communication of Electronic Protected Health Information by E-mail)**

a) The transmission of EPHI from Washington University to a patient via an email or messaging system is permitted if the sender meets the following conditions are met:

- The patient has been made fully aware of the risks associated with transmitting EPHI via email or messaging systems.
- The patient has formally (written) authorized Washington University to utilize an email or messaging system to transmit EPHI to them. The patient's authorization should give explicit permission to copy (CC:) other recipients, if this is required.
- The patient's identity has been authenticated (see above).

b) The transmission of EPHI from Washington University to an outside entity via an email or messaging system is permitted if the sender meets the following conditions:

- The receiving entity has been authenticated.
- The receiving entity is aware of the transmission and is ready to receive said transmission.
- The sender and receiver are able to implement a compatible encryption mechanism.
- The entire message or all attachments containing EPHI are encrypted.

c) The transmission of EPHI within Washington University (including WUCON, WUSTL and CARENET domains) (See HIPAA Security Policy #13 - Access Control, paragraph #3) using an email or messaging system is permitted without additional security measures for a minimal amount of EPHI that is not high risk, sensitive or critical. Use an encrypted or password-protected attachment to send high risk, sensitive or critical EPHI.

d) Email accounts that are used to send or receive EPHI will not be forwarded to non-Washington University accounts. A departing staff member who remains part of the workforce must utilize a secure access method (VPN, etc.) for remote access to email and other resources.

3) EPHI Transmissions Using Electronic Removable Media

a) When transmitting EPHI via removable media (for example: floppy disks, CD ROM, memory cards, magnetic tape and removable hard drives) the sending party must:

- Use a data encryption mechanism to protect against unauthorized access or modification
- Authenticate the person or entity requesting said EPHI in accordance with HIPAA Security Policy #16- Person or Entity Authentication)
- Send the minimum amount of said EPHI required by the receiving person or entity. (See HIPAA Privacy Policy # 11 - Minimum Necessary Request, Use or Disclosure of Protected Health Information)

b) If using removable media for the purpose of system backup/disaster recovery and the removable media is stored and transported in a secured environment, no additional security mechanisms are required. If using removable media for file transfer within a secured physical environment, no additional security mechanisms are required.

4) EPHI Transmissions Using Wireless LANs and Devices

a) The transmission of EPHI over a wireless network within the Washington University (WUCON and .wustl.edu) domains is permitted if the following conditions are met. All Radiation Oncology managed wireless networks do/will comply.

- The local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized.
- The local wireless network is utilizing an encryption mechanism for all transmissions.

b) If transmitting EPHI over a wireless network that is not utilizing an authentication and encryption mechanism (or you are not sure), encrypt the data before transmission using a mechanism described in "Security Measures", above.