Washington University in St. Louis

HIPAA Privacy Procedure #17-6

Effective Date: April 14, 2003
Reviewed Date: February, 2011
Revised Date: March, 2007
Scope: Radiation Oncology

Electronic Sharing/Transmission of Data Containing Protected Health Information

****

Policy Expectation:

Protected Health Information (PHI) should only be shared with authorized parties, in accordance with all applicable laws, rules, regulations, and Washington University (WU) policies. When electronically transmitting PHI to locations outside of a secure network, a mechanism for maintaining integrity and confidentiality during transmission must be employed.

Why is this important?

- Ensures that electronically delivered PHI is not subject to eavesdropping while crossing unsecured networks.
- Minimizes the potential for PHI to be altered during its traversal from source to destination.
- Failure to comply may result in WU being liable for civil or criminal penalties under HIPAA regulations.

What do you need?

- Copy of WU HIPAA Policy on Security Measures Required to Comply with Privacy Policies.

Steps:	Additional Information
1. Electronic Sharing/Transmission of Data Containing Electronic Protected Health Information PHI should only be shared with authorized parties, in accordance with all applicable laws, rules, regulations, and WU policies. When transmitting PHI electronically outside of a secure network, one of the following methods should be used: • Virtual Private Network (VPN) tunnel • File encryption/decryption (e.g. PGP encryption) • Secure Socket Layer (SSL) encryption	

2. If the transmission of PHI is to a destination located within some other secure network, a virtual private network (VPN) connection may be required. Once the VPN connection between the Business Unit and the remote network is established, the transfer of PHI may be executed by any mechanism except **via electronic mail.**	This may also require you to install special software and request a username and password from the destination's networking organization. Refer to WU HIPAA Policy on Security Measure Required to Comply with Privacy Policies. If you have any questions you can contact the Rad Onc Security Liaison – Chris Alexander – Security Liaison (362-9741)
3 If the transmission of PHI is to be a destination that is NOT located within some other secure network, an appropriate encryption mechanism must be coordinated with the recipient as follows: a. Files transferred via an unsecured mechanism such as Windows file sharing, NFS, or FTP must be encrypted prior to transmission using a public key encryption mechanism and the recipient's public key. b. Transferring PHI through a web interface must utilize secure socket layer encryption (SSL). c. Email containing PHI must be encrypted during transmission (except as noted in Step 1)	A browser will indicate a secured session by displaying a lock icon (or something similar) in its status bar. Many email systems allow the user to select whether a message will be encrypted prior to delivery. If the email system does not provide this option, encrypt the PHI as described above and attach the encrypted file to the message before sending.
4. Review process to ensure that the process for sharing PHI electronically is carried out in accordance with both the pertinent WU HIPAA policies and this Business Unit procedure.	Radiation Oncology HIPAA Security Liaison will review these procedures with the radiation oncology HIPAA security committee. Periodic surveillance may be used by Information Systems to insure compliance. Chris Alexander – Security Liaison (362-9471)