Washington University in St. Louis

HIPAA Privacy Procedure #17-4

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

Passwords

****

Policy Expectation:

Protected Health Information (PHI) should only be accessed by authorized parties in accordance with all applicable laws, rules, regulations, and department policies. Protection of electronic data containing any element of PHI should follow the “2-key” concept. The 2-key concept has been generally applied to all secure PHI data repositories, whether physical or electronic, and should be maintained for all electronic repositories to ensure necessary data protection and security of PHI.

Why is this important?

- Ensure that PHI can only be electronically accessed by authorized parties.
- Failure to comply may result in being liable for civil and criminal penalties under the HIPAA regulations.

What do you need?

- Security Measures Required to Comply with Privacy Policies (including Attachment A)

Steps:	**Additional Information**
1. Database custodians (or network administrators in the case of network authentication) are responsible for determining the level and type of password necessary to appropriately secure the PHI contained within the repositories they are responsible for.	The custodian should identify which method of password management (static or periodic changes) they have in place for their databases when completing the annual Departmental Database Registration (see HIPAA Procedure #17-2 Attachment A)
2. Passwords should be a minimum of six (6) alphanumeric characters in length for best practice security purposes.	Legacy systems may not be able to accommodate six-character passwords.

3. All user-level passwords should be in accordance with the guidelines below. ➢ Passwords should not be a word that can be identified in the dictionary. ➢ Password should not be the name(s) of children, pets or other items that can be easily identified with the user. ➢ Do not write down the password and keep it in a visible location within the work area. ➢ Do not share the password with anyone. ➢ Passwords should not be reused within 3 iterations. ➢ Intrusion detection is recommended. 4. Whenever possible, systems should force input of a new password after the prescribed time interval has passed. 5. The Radiation Oncology Security Liaison should review procedures annually with the Radiation Oncology system managers to insure that all systems are managed according to department procedure. 6. Security breaches are subject to disciplinary action, up to and including termination. Infractions should be brought to the attention of user, supervisor, and Division management for appropriate action.	Examples of system-level passwords include root, enable, NT administration and application administration accounts.