Washington University in St. Louis

HIPAA Privacy Procedure #17-3

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

Access to Electronic Protected Health Information

****

Policy Expectation:

Protected Health Information (PHI) should only be accessed by authorized parties in accordance with all applicable laws, rules, regulations, and department policies. Data custodians will be responsible for PHI access and must determine, track and monitor who has access to PHI.

Why is this important?

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

What do you need?

- Copy of HIPAA Policy on Security Measures Required to Comply with Privacy Policies
- A custodian assigned the responsibility of securing the PHI and administering PHI security

Steps:	**Additional Information**
1. Access to PHI is available through the database custodian with overall security responsibility for each PHI repository.	The PHI custodian must assign access for each authorized individual. This may be delegated to security administrators through a formal security access request process. Each access request should be explicitly authorized in writing or by email by the PHI custodian or delegate. Access will be assigned based on job classification. The PHI custodian or delegate will assign passwords and will maintain a record of passwords assigned and level of access assigned.
2. Database custodians assign access to PHI in a repository based on the individual's job function and access requirements.	Refer to HIPAA Policy/Procedure on Minimum Necessary Request, Use or Disclosure of Protected Health Information.

	If multiple users access an electronic PHI repository and have no reason to regularly access all of the data in a repository, the custodian should ensure that the data repository is configured in such a way that access rights can be distinctly tiered for different levels of access. If an individual requires access to a PHI repository infrequently, access should be assigned temporarily, and then revoked when the access is deemed no longer required. Temporary access, such as for residents rotating from another institution or for visitors, will be time dependent and will be revoked at the end of the period.
3. Database custodians will regularly review access privileges to the PHI repository for all individuals with access to the PHI based on their business needs. Access will be revoked for those individuals with access to the PHI repository that have subsequently been terminated or have subsequently transferred to an area where access to the current PHI repository is no longer needed.	Access for those individuals with more pervasive or super-user type access to the PHI data (e.g. administrators) should be reviewed with more frequency. Off-staff notices will be routinely sent by the department payroll office to IS system administrator and to Physics custodian. Payroll will also send off staff notice to Radiation Oncology Privacy Liaison, who will forward to all repository custodians of multiple-user repositories. If access to a different PHI repository is required, access should be assigned by that repository's custodian.

4. The system administrator or custodian will determine if the repository is a high-risk PHI repository	A high-risk PHI repository would include: • PHI repositories that are enterprise-wide in nature. • PHI repositories that contain data on a large number of individuals. • PHI repositories accessed by a large number of the Workforce.

5. The system administrator or custodian will maintain a log of all access to PHI repositories classified as high-risk. This log will be required if: there is no authorization or access is not for purposes of treatment, payment, or operations. This log may be on paper or may be electronic or may be an Excel spreadsheet.	The log should record at least the name or ID of the WU workforce member who accessed PHI, the PHI repository accessed, and the date/time. Risk classification will be done by Dept. Security Stakeholder Group. See Accounting Procedure #3.
6. The RO Privacy Liaison will annually review repository registrations and randomly interview custodians regarding repository usage. This interview may involve review of user logs. The RO Privacy Liaison will investigate any reported infraction of the Access to Electronic PHI policy and report results to the ROC HIPAA Security Stakeholder Committee.	

Exhibit A

PHI Repository and Access Log

NAME	Title/Function	Access Paper(P) Electronic (E)	Limits of Access

Signature of Staff Person _____

Date: _____

Print Name and Title: _____