School of Medicine and Public Health
UNIVERSITY OF WISCONSIN-MADISON

HIPAA Security Policy

Policy Title:	Accounts, Access and Auditing
HIPAA Policy Reference:	5.2
Effective Date:	September 1, 2011
Status:	Revision

1. Purpose

Under HIPAA, access to PHI must be restricted to authorized individuals and a historical record of that access must be kept. For PHI in electronic form this is done by use of individual authenticated accounts, control of access to PHI for each specific account, and tracking the use of all accounts. This policy addresses authentication of individuals, account creation and deletion, authorization of data access for accounts and tracking of access.

2. Definitions

2.1. *Basic Access Controls:* Mechanisms used to control access to a dataset based on user name or group membership

2.2. *Full Access Controls:* Mechanism used to control access to specific individuals with all access being recorded for audit purposes.

2.3. *Account Requestor:* Administrative authorities designated by the department to make requests that a login account be created or terminated, or that account access be changed.

2.4. *Account Holder:* Individual authorized to access a particular database containing PHI.

2.5. *Auditing:* The retrospective review and reporting of access to electronic records.

2.6. *Abandoned Account:* An account that has not been used for a substantial period of time and is no longer needed, as determined by departmental policy.

2.7. *Dataset Custodian:* The individual or entity who is accountable for research uses of a dataset.

2.8. *Dataset Administrator:* The departmental IT person or group responsible for maintaining access controls to a dataset.

3. Policy

Account Creation, Deletion and Management

Computer user accounts are the first perimeter of access to PHI, and as such, the policy goal for their management should be the same as the goal for managing access controls. The following policies apply to login and other accounts (e.g. database accounts) used to control access to PHI.

3.1. Access to PHI must be restricted by the creation of user login or database accounts which limit access to those individuals who are authorized to change and/or view the data to carry out the duties of their job. A historical record must be kept of all account changes for a period of at least six years.

3.2. Account holders must complete all applicable SMPH HIPAA training before accessing PHI.

3.3. Account request procedures should enumerate additional information as needed at the time of creation to limit access. If the creation of an account automatically allows access to a PHI dataset, the dataset custodian must authorize the account through appropriate departmental IT.

3.4. If an account is known to be temporary at creation, an end date must be specified.

3.5. Periodic scans for abandoned accounts should be performed and appropriate action taken.

3.6. Departmental IT staff must be promptly notified by the Account Requestor of any change in status of an account holder that may affect their access rights, including their right to hold an account.

3.7. Accounts may be terminated in accordance with guidelines defined by the department, e.g.

- The Account Requestor specifies that the account be terminated,
- The account has been determined to be abandoned,
- The account holder has violated HIPAA policy

Access Control

3.8. All datasets containing PHI must be protected by one of the following types of access controls. The type of access control must be appropriate for the characteristics of the dataset.

- Locked room and login where no other method is practical, e.g. lab computers,
- Basic access controls for simple aggregations of files containing PHI, e.g. datasets on spreadsheets and single-user or lab databases,
- Full access controls for large multi-user PHI databases where mechanisms to control access and audit from within the database is appropriate.

3.9. Only Dataset Custodians may grant someone else access to their dataset and must do so by notifying the Dataset Administrator.

3.10. Account holders are responsible for determining whether or not they store a significant amount of PHI on a department's network or servers. If so, the account holder must notify the departmental IT group and act as the Dataset Custodian.

3.11. If the Dataset Custodian wants to delegate custodianship to one or more proxies, he or she must notify the Dataset Administrator in writing.

3.12. Upon termination of an individual's appointment, all associated user accounts, services, and resources, must be revoked as soon as possible, preferably the day of termination, but in no event later than three (3) business days following any such termination.

Account and Access Auditing

Access to datasets containing PHI must be tracked at some level depending upon its size and complexity. As a dataset grows and access rights change, the dataset custodian and department IT will periodically reevaluate the appropriateness of technologies and procedures, and will make changes accordingly.

3.13. All accounts must be tracked with a history of creation, modification or deletion kept for six years.

3.14. The Dataset Administrator should maintain an account and access record for all account holders having access to each PHI dataset.

3.15. The level of auditing of each of the databases must be related to the level of risk of unauthorized access. All datasets will be categorized as being level 1, 2 or 3 based on several criteria:

- Level 1 contains a large amount of data from many individuals most of which can be accessed from a large number of staff in the department or from outside the network on which it resides (this describes clinical trials in many cases). Auditing must be done at as high a level as possible, preferably record logging,
- Level 2 contains significant amount of data from several individuals some of which is accessible to a segregated group of users; clinical laboratory databases would be an example. At minimum it is required to record log-in activity for each account with access,
- Level 3 contains a limited amount of PHI that can be accessed by a very limited number of individuals and is not accessible outside the network on which it resides. Logging must at minimum consist of a time history of accounts with access to this database.

4. Departmental Procedures

4.1. The departmental IT group must provide a method for securing PHI, either by:

- Treating all of that user's data as PHI and securing it accordingly or
- Offering the user a storage method by which the PHI can be segregated and protected appropriately

4.2. Each department must have written procedures to be used when creating login and database accounts on computer systems that contain or may allow access to PHI. The procedures must include:

- How accounts are authorized, who creates them and what information is required before an account is activated
- What, if any, access rights are given by default
- Description of forms (electronic or paper) used
- Procedure for account deletion

4.3. Each department must keep account and access records for all datasets that have resided on its computers for six years. For smaller datasets, these records comprise its audit record (See Audit Controls Policy).

4.4. Each department must keep a list of PHI databases and the mechanism used for auditing each dataset. Logs must be reviewed periodically by the department for unusual activity. If inconsistencies are found, departmental IT staff must work with the dataset custodian to remedy the situation as promptly as possible.

5. References

5.1. Related HIPAA Security Policies

- Password Use and Storage
- Server Security

5.2. UW Health Policy 1.02: Access to Electronic Information Systems