School of Medicine and Public Health
UNIVERSITY OF WISCONSIN-MADISON

HIPAA Security Policy

Policy Title:	Password Use and Storage
HIPAA Policy Reference:	2.2
Effective Date:	September 1, 2011
Status:	Revision

1. Purpose

Access to PHI must be restricted to authorized individuals only and in most cases passwords are used as the credentials to identify those individuals. This policy assures the appropriate use of passwords to ensure data security.

2. Definitions

2.1. *Strong Password:* A password that is sufficiently long and complex to make it difficult to detect by both humans and computer programs. For example, passwords that comply with the UW-Madison Password Policy (reference 5.3) are considered strong.

3. Policy

Each user who needs access to PHI will be given an individual account which will require authentication by some means which could include user name and password. Treatment of a password must follow these restrictions:

3.1. Sharing of accounts or divulging your password to anyone else is prohibited. If a situation exists in which sharing of passwords appears unavoidable, (e.g. with dedicated laboratory equipment) departmental IT staff must be consulted and special measures will be taken to provide alternate appropriate security (e.g. a locked and monitored room).
3.2. When a new account is created, a temporary strong password will be issued to the user. The user will replace the temporary password at the subsequent login.
3.3. Any passwords used to access PHI must be constructed in such a way to be considered strong.
3.4. Passwords are not to consist of proper names, initials, email addresses or dictionary words.
3.5. Passwords must be stored securely. Writing passwords down should be avoided, but if necessary they must be stored securely, for example, in a locked drawer. Passwords may be stored on an electronic portable device only if reliably encrypted. It is the responsibility of the employee to ensure secure storage of all passwords issued to them.
3.6. If you suspect that your password is being used by someone else, you should report it to your departmental IT support person immediately. Standard passwords must be changed at least every two years. Passwords used for administrative accounts on servers must be changed at least every 180 days, or immediately upon termination of a departmental IT staff member's administrative responsibility.

4. Departmental Procedures

Each department must maintain written procedures to describe the following:

4.1. How passwords are administered, including password validation and aging. The procedure should be technically enforced when possible. Periodic password security audits are recommended.
4.2. A list of administrative passwords held by departmental IT members and the computer to which each password grants administrative access.

5. References

5.1. Related HIPAA Security Policies
- Workstation Use and Security
- Server Security
- Account Creation, Access Control and Auditing

5.2. SANS Policy: http://www.sans.org/resources/policies/Password Policy.pdf

5.3. UW-Madison Password Policy: http://www.cio.wisc.edu/policies/password.aspx