

University of Wisconsin-Madison
HIPAA Security Best Practices Guidelines
#2

1. Guideline Name: **Account Creation and Access Control**

2. Definition and Purpose:

A. **Purpose** The purpose of this policy is to provide suggestions, based on current best practices, for creating user accounts on and defining access control to computer systems. The intention is to reduce the risk of data access by unauthorized people.

B. Definitions

1. **HIPAA** (Health Insurance Portability and Accountability Act): A set of standards for the security of electronic protected health information that by health plans, health care clearinghouses, and certain health care providers must implement.
2. **PHI** (Protected Health Information): Any information (such as a name, address, photo, etc.) that identifies real people in a health care setting.
3. **Access Control**: The act of limiting a user's access to certain data or files based on role or job function.
4. **Account Creation**: This is the process of creating an account (or some other access point) on a computer system and granting it permission to access or use some subset of files or data. Security policies developed by the organization should govern this process. The policies should not only address the creation of the account, but should also address how long the account exists and describe the conditions in which the organization terminates the account.
5. **Data "Browsing"**: The act of viewing data or records not directly within the scope of one's job functions at the time. For example, a health care provider looking at records of patients not under that provider's care.
6. **Access Level**: The "rights" a user account has concerning access to a file or data. These will vary among operating systems, but usually include: *read* (the ability to look at a file or its contents), *write* (the ability to create a file or modify an existing file's contents), and *delete* (the ability to erase a file).

3. Reference to HIPAA Standard:

A. **HIPAA**: The suggestions in this policy address the concerns found in the following HIPAA sections: §164.308(a)(4), §164.308(a)(8), §164.312(a), and §164.312(d).

B. **Other Policies**: The reader may benefit from a review of the following related policies.

1. UW-Madison "Appropriate Use" policy (http://www.doit.wisc.edu/security/policies/appropriate_use.asp)
2. Password Management (Best Practice Guideline #6)
3. User Authentication (Best Practice Guideline #4)
4. Audit Controls (Best Practice Guideline #3)

4. Description of Best Practice Guideline:

A. Account Creation: A true "best practice" guideline was difficult to find on the web. The author offers the following suggestions for a policy template, based on examples found at the web links referenced in section 5.1.1.

1. This guideline directs the following recommendations to those to create user accounts on computer systems. Some applications (such as large database systems) may use their own accounts in addition to (or in place of) the operating system's accounts. Administrators of such systems may want to use these recommendations for creating application-level accounts.
2. The account creation policy should define who is eligible for an account. Only those who need access as part of their job responsibilities are eligible.
3. The policy should also describe the procedure for requesting an account. Typically, an administrative authority (such as a supervisor or a personnel office) should write such a request.
4. The supervisor, appropriate administrative manager, and data custodian require signature approval.
5. The name of the account (usually, the employee's username) must be unique within the organization.
6. The System Administrator should assign an initial, strong password to the account, and configure the account so that the employee must change the password (using strong password guidelines) at the first login.
7. The policy should define the duration of the account. Usually this is the employee's employment period.
8. Finally, the policy should define or explain the conditions in which the organization deletes the account. One obvious condition is that the account expires when the user or organization terminates employment. Other conditions may include use of computers for personal tasks, inappropriate web browsing, illegal activity, data "browsing," or other non-work related activity.

B. Access Control: By carefully setting access controls, you can reduce both intentional and unintentional security breaches. For example, denying read access helps to protect confidentiality of information, and denying

unnecessary write (modify) access can help maintain the integrity of information. Limiting the execution privilege of most system-related tools to authorized system administrators can prevent most users from making configuration changes that could reduce security. It also can restrict the ability of intruders to use those tools to attack the system or other systems on the network.⁽⁺⁻⁾ You will also mitigate security breaches by using audit controls that come with most operating systems, or that may be available commercially, and periodically reviewing the audit logs.

1. Although this guideline directs the following recommendations mostly at files, you can apply these concepts to large application systems that manage access control to their own data. For example, a database application that uses several tables may have mechanisms within it that allow an administrator to determine which users (of the application) have access to particular columns or tables. So, one can approach access control to such a system from a "file" view or from an "application" view.
2. Choose a file system that lets you define access rights. For example, the Windows FAT file structure does not have any built in security features; the NTFS structure does. You should move PHI to systems that use file/folder rights to determine access.
3. Identify files and folders containing PHI, and list those people authorized to use it and their access level. A good way to separate rights for PHI versus non-PHI files is to create a matrix listing file categories (PHI being one category) on one axis and users or user groups on the other axis. At each file/user intersection record the appropriate rights.
4. Create user groups, and assign rights to PHI files to groups, where possible, rather than individuals. This will help simplify access control. However, be sure that all of the members of each group really do have the same permission to access files as the group. Making a user a member of a group may unintentionally give rights to PHI or files that user may not normally have. If there is a contradiction between access rights to PHI and group membership, either create a different group or assign rights to individual users.
5. Configure access control to PHI and other files.
 - a. Assign rights (read, write, delete, other) to groups or users as appropriate.
 - b. Disable write access to executable or binary files.
 - c. Restrict access to operating system files to the "read" level, if possible.
 - d. Using access control, try to prevent users from installing software, scripts, or other executables. Using access control, try to prevent users from installing software, scripts, or other executables.
 - e. Be aware of rights inheritance. Rights given to a group of users in one folder may not be appropriate in subfolders. Many operating systems by default allow subfolders to inherit rights from parent folders.

6. If possible and warranted, apply encryption to files containing PHI. Be careful when using file encryption. Operating systems sometimes relate encryption keys to user accounts. If you delete those accounts (when the user leaves), you may lose the ability to decrypt files.
7. Document access control rights, and review the documentation periodically. Update the documentation whenever rights change, you add new users, or you delete old users. Include not only the users/groups and the rights given to files, but also the rationale for assigning or denying certain rights.

5. Reference Documents and Websites:

A. Account Creation

The web sites below display account policies from different institutions of higher education. The CERT link lists some general "best practices" for accounts and passwords.

1. <http://www.itc.virginia.edu/policy/accounts.html>
2. http://www.eleceng.ohio-state.edu/computing/ER4_accounts.html
3. <http://www.cert.org/security-improvement/practices/p069.html>
4. <http://campus.northpark.edu/cs/account/creation-deletion.htm>

B. Access Control

1. <http://www.cert.org/security-improvement/practices/p029.html>
2. <http://www.cert.org/security-improvement/practices/p070.html>
3. <http://www.itsc.state.md.us/info/InternetSecurity/BestPractices/AccessControl.htm>

6. Document Revision History:

Task	Date Completed	Author
Document Created DeMuth	9/18/03	John M.
Format changes per 9/24/03 meeting. DeMuth	10/24/03	John M.
Content changes as recommended by J. Caruso and DeMuth K. Milford.	10/27/03	John M.
Added minor text that applies guideline to applications DeMuth that manage their own data (D. Miran); reference to "Proposed Guidance for Access Authorization" document (M. Wood, P. DeLuca); references to auditing (general discussion) per 11/12/03 meeting.	11/14/03	John M.