Selecting Strong Passwords (HIPAA on the Job)

by Margret Amatayakul, RHIA, FHIMSS, and Tom Walsh, CISSP

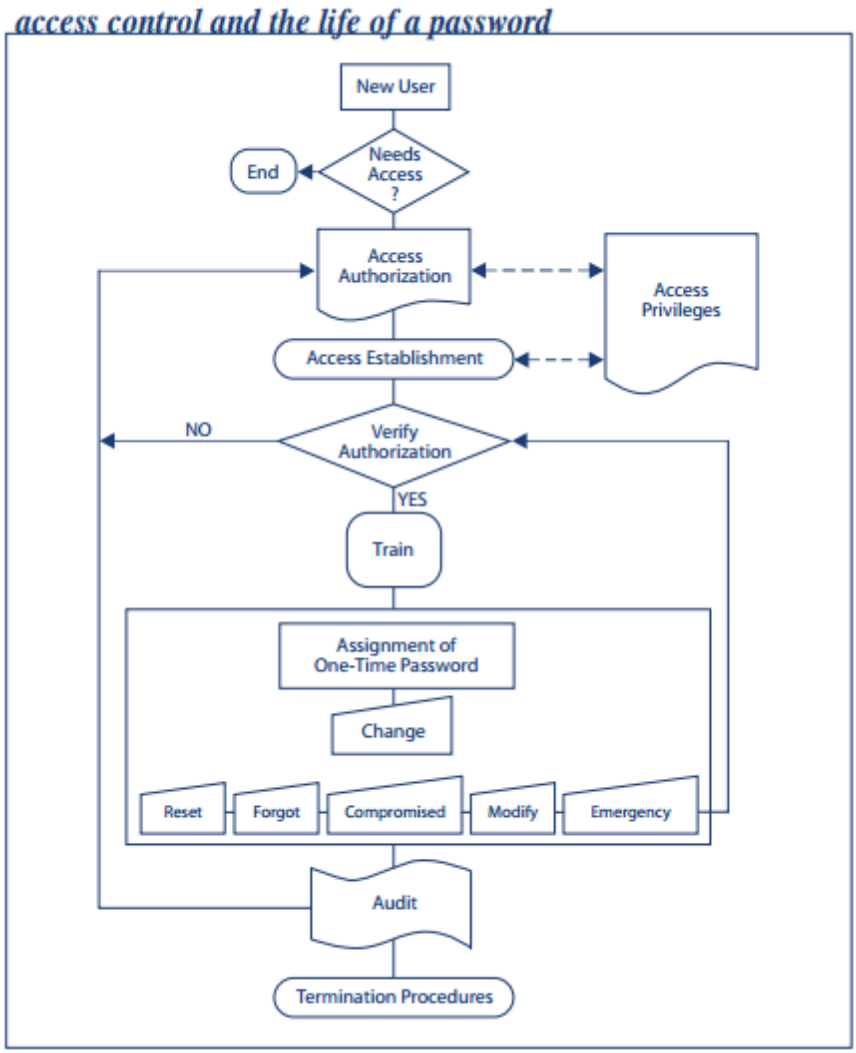
Are the majority of passwords in your organization something like “Spot1,” “Spot2,” “Spot3” (for Joe, whose password expires every 90 days and whose dog’s name is Spot)? If so, your organization could be at risk. Here’s what you need to know about HIPAA requirements for establishing and managing passwords.

What Does HIPAA Require?

HIPAA requires a two-tier form of entity authentication. Entity authentication is defined as “the corroboration that an entity [person or system] is the one claimed.” A unique user identifier and one of the following are required: biometric identification (such as fingerprint or retinal scan), password, personal identification number (PIN), telephone call-back procedure, or token. Most healthcare vendors provide a unique user identifier and a password. However, the system with which passwords are administered and passwords themselves are not as strong as they could be. A strong password is easy for the user to remember and difficult for anyone else to guess.

What Is Entity Authentication?

The whole process of entity authentication includes **definition of access privileges, access authorization, access establishment (including verification, training, and assignment of authentication), password management, and audit controls**. Access control should also include modification of access when a user changes jobs within the organization, emergency-mode access, automatic log-off, and termination procedures to ensure access is removed when a user terminates association with the organization. (“Access Control and the Life of a Password,” below, illustrates these steps.)



What Are Access Privileges?

Access privileges should be defined at the time a system is installed. HIPAA permits one of the following:

- **User-based access control** identifies the user to the system, and the user has access to all information. Many hospitals grant physicians user-based access controls on the premise that, in an emergency, a physician should not be restricted from accessing any information. Such access privileges, however, can be improved through the use of emergency-mode access controls, also required by HIPAA. These controls limit access only to information in which the user is a user of record but permit access to other information when there is a demonstrable need for access.
- **Role-based access control** assigns privileges based on the role of the user. A nurse on one unit may be able to access records of only the patients on that nursing unit. A laboratory technician may be able to view all patients in-house but may not write to any record except in the laboratory information system. Most vendors supply some form of role-based access control today and are looking to enhance this for HIPAA.
- **Context-based access control** assigns privileges based on a much more detailed level. It controls access to given data elements and will change the level of access based on the role being assumed at a given time. For example, a nurse in the emergency department may have access to all patients' medication histories but not to detailed reports of histories and physical exams.

The American Society for Testing and Materials' (ASTM) E1986 Standard Guide for Information Access Privileges to Health Information further clarifies these access levels and recommends that both data elements and healthcare personnel warrant differing levels of access control.

How Is Access to Information Controlled?

Once access privileges are defined, HIPAA's information access control requirements describe how access is authorized, established, and modified. Access authorization policies and procedures should require manager approval for assignment of a specific access privilege. Access establishment policies and procedures commonly require a controlled number of individuals who may receive the access authorization and assign access rights. The process should entail:

- **Verification** of the individual to whom the access is granted. There should always be a positive form of identification made before assigning a password. If a password is not assigned in person with a photo ID, then some other system, such as a secret question and response, should be used to verify identity.
- **Training** in selection of passwords and other aspects of workstation use. This should be performed at the time access is established. In addition to selecting a strong password, users should be trained in virus protection, to monitor for unsuccessful log-ins, and how to report security incidents.
- **Assignment** of a one-time password that permits access to the system and creation of the user's own password. Today, many systems assign a default password that allows users to use the password several times, if not indefinitely. Time is critical in a healthcare environment, so it may be appropriate to set the initial password to a two-time use, but retaining this password beyond that is extremely risky.

Access modification policies and procedures apply when a user changes jobs or believes a password has been compromised. Access modification requires coordination between transferring managers.

What's the Best Way to Choose a Password?

In evaluating the options permitted for the second tier of entity authentication (in addition to the unique user identifier), the password is the most common. A PIN is typically considered the weakest. Biometrics and tokens are considered the strongest, but they are also the most expensive. Telephone callback is generally inconvenient and not totally reliable. Good business practice suggests that a password would be adequate authentication as long as there is strong password management (as described above) and:

- self-selection of a strong password
- controlled frequency of change of password
- passwords should not be reused
- same password for multiple applications/systems per user

Selecting a strong password is something users should be taught to how to do. The password characteristics should match the operating system requirements. For example, under Windows 95, 98, and NT, passwords of seven characters are best because of the way Microsoft stores the password. UNIX passwords are best at eight characters; in fact, additional characters in the UNIX password are ignored.

Passwords made up of alphabetic, numeric, and special (if possible) characters in upper and lower case (if possible) are best. These passwords should be easy to remember and difficult for others to guess. Some suggestions include:

- two short, disassociated words combined with or containing special characters and upper- and lower-case characters (for example, k!s$rugS [kiss rugs])
- a short phrase spelled in a unique way (for example, buy3w@y [by the way])
- a mnemonic, also including numbers and special characters (for example, Owt$gm1 [Oh When The Saints Go Marching I(1)n])

Avoid using:

- words that are easy to guess (for example, "Cubbies," for a baseball fan who lives in Chicago)
- words that convey personal information (for example, license plate, spouse name, or other identifier typically associated with an individual, such as a unique physician identification number or an employee's badge number)
- single words found in a dictionary of any language
- repeat characters (for example, AAA222)

Information security professionals disagree on the exact frequency with which passwords should be changed, but they do agree that the stronger the password, the less frequently it needs to be changed. The environment may dictate frequency, but six months to one year can be appropriate for many organizations, as long as the password is strong.

Ideally, a "single sign-on" system would authenticate users to all applications to which they have access privileges, making it necessary for users to have only one password. Because of the potpourri of systems in hospitals today, a single sign-on is not totally feasible. Therefore, users should be encouraged to use the same password for every application/system to which they have access.

While there is a risk that one compromised password would compromise all systems, it is more likely that one remembered password would be less frequently compromised than many passwords that cannot be remembered and have to be recorded somewhere. To the extent possible, users should not be able to reuse passwords once they have changed the password.

Some schools of thought encourage the subsequent password to be a spin-off of the first, such as changing one number in sequence, again to promote memorization. Others consider this to be too close to not changing the password at all and encourage an entirely different password. The likelihood of password compromise should dictate recommendations concerning password construction.

Automatic log-off of systems after a set period is also associated with password management. HIPAA requires automatic log-off but does not specify the time. Each organization should evaluate the location of the workstations and set times that reflect the risk of inappropriate access.

What Are Audit Controls?

Some information systems specialists suggest that strong access controls negate the need for audit controls. While the prevention afforded by access control is better than the remediation provided by audit controls, audit controls are a requirement under HIPAA and a key element in supporting access controls. Audit controls, including audit trails, ensure that access controls work. They provide proof of access that may be allowed based on the access privileges, but is inappropriate.

How Should I Handle Sanction Policy and Termination?

The proposed security rule defines sanction policy as "such policy regarding disciplinary actions which are communicated to all employees, agents, and contractors, for example, verbal warning, notice of disciplinary action placed in personnel files, removal of system privileges, termination of employment and contract penalties."

The rule references ASTM standard E1869 (Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Computer-based Patient Records). E1869 states that "All organizations and individuals shall adopt and use sanctions to deter inappropriate access, misuse of data, unauthorized release of data and sharing of access mechanisms." It further indicates that "Intentional violations should be penalized more severely. Response to negligent, inadvertent, or accidental violations should include the reeducation of the individual as well as a review of related policies and procedures. Penalties should be adjusted to fit the situation ranging from dismissal from the job or loss of contract to lesser sanctions."

HIPAA also requires formal, documented instructions, including appropriate security measures, for the termination of a user's access. Whether friendly/voluntary or unfriendly/involuntary, all terminations should be treated equally.

Because a number of parties (including management, human resources, payroll, and information systems) are often involved in a termination, a system of checks and balances is needed to ensure that all parties have performed their tasks on time. The manager should be responsible for the initial notification and verifying removal of access. For employees, an automatic link between processing the last paycheck and access removal would be desirable. If this is not possible or not reliable, it is advisable to purge accounts after a defined period of inactivity.

Managing termination of access for agents and contractors is always more difficult, but it can be the weakest link. Agent or contractor access can be controlled by setting up their access accounts to automatically suspend on the date their contract ends and by assigning them unique user identifications that can be easily tracked for activity (for example, all temporary unique user identifications begin with the letter T). A list of unique user identifiers with active accounts should be generated regularly

and used by applicable parties to validate continued requirements for the account. Any changes or terminations that have not been removed will appear on the list.

***Margret Amatayakul**, RHIA, FHIMSS, is president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL. She can be reached at margretcpr@aol.com. **Tom Walsh**, CISSP, is practice manager, enterprise security, for Healthcare Computing Strategies, based in Wheaton, IL. He can be reached at trwalsh@hcs-is.com.*

Article citation:
Amatayakul, Margret. "Selecting Strong Passwords (HIPAA On the Job series)." *Journal of AHIMA* 72, no.9 (2001): 16A-D.
