Codify
BY AAPC

Health Information Compliance Alert

Security Compliance: Identity & Authenticity: A Dynamic Duo You Need To Meet

Use these tools to ensure your security rule compliance.

The HIPAA security rule not only demands that you develop procedures to identify people with access to your patients' PHI. It also mandates that you authenticate that access. But what does that really mean for you?

Who Has Access?

Identity is "the determination that a person, role, server or device actually exists," explains **Sean Steele**, director of business development for **Tovaris**. "When you identify something or someone, you are saying that the entity is valid and current for your organization's purposes," he says. Example: Joe is identified as a valid user on this network.

"You use identity to grant access," explains **John Burdick**, president of Altamonte, FL-based **eMed Systems Group Inc**. A person's identity tells your system who is allowed to access PHI and at what level, he says.

How Do We Prove It?

While a person's identity tells you they can access PHI, that person must also provide proof they are who they purport to be, experts say. This is where authentication comes in.

"Authentication is the process or method of confirming a user's identity," Steele defines. With escalating incidents of identity theft, being able to authenticate that your users really do have access rights to your network is crucial.

Your users can authenticate their identities by providing:

- something they know, such as a password or identification number;
- something they have, such as a token or badge; or
- something that is part of the user, such as a fingerprint.

However, "the strongest authentication involves a combination of these techniques," Steele advises.

Example: Joe authenticates himself to the network using a three-factor login -- his password, a secure badge and his right index fingerprint. An ATM uses two-factor authentication: your ATM card and your 4-digit PIN, Steele reminds.

How Do They Work Together?

Identifying your users and providing them with multiple ways of authenticating that they are who they say they are will strengthen your system against both internal and external attacks.

And, considering the size of your organization, you don't have to stop at one password, Burdick reminds.

Tip: "Layer passwords so that users must identify and authenticate themselves in multiple ways as their level of access to information increases," he counsels. Example: Give Joe one password for entering the system, one password to access

certain files and still another password for modifying those files, Burdick explains.

Problem: However, if you have a large number of users who must be identified and authenticated, layered and unique passwords could prove risky. It can be inconvenient and "users will probably attempt to circumvent the authentication process if they become frustrated," Steele warns.

Solution: Control this problem by using a management infrastructure like single sign-on, Steele recommends. This allows users to "sign on once to use multiple applications and resources over the course of a workday," he explains. This type of control system will also help you manage the cost of password implementation and maintenance, he says.

Remember: The most important part of authentication is "placing restrictions that are unique to each user so that no one can duplicate them," says **Sarah Elliot**, an attorney at **von Briesen & Roper** in Milwaukee, WI.

The Bottom Line

Identification and authentication rely on each other and both are necessary to keep your patients' PHI secure.

Here's a good working definition of the terms: "Identification shows this person is authorized to access the information in your system. Authentication is how they prove it," explains **Dennis Bagley**, manager of health care and technology consulting at Southfield, MI's **Plante & Moran**.

Whether you implement layered passwords, single sign-on or another type of access management system, effective identification and authentication policies will secure your patients' PHI against inappropriate access. By identifying which people should be accessing your network, and providing them with the keys to prove who they are, you are saving your organization from a HIPAA violation.