Codify
BY AAPC

Health Information Compliance Alert

Compliance: Pocket These Password Tips to Protect Your Practice

Hint: Multi-factor authentication helps thwart hacks.

Technology is a valuable tool for getting the job done in the healthcare industry today. But if you don't take precautions to keep data safe, your organization could end up in hot water.

Fortunately, there are strategies that you can employ to safeguard your mobile devices and workstations as well as your patients' electronic protected health information (ePHI). Comprehensive training on passwords and best practices are the foundation for protecting your organization against a cyber attack.

One of the best ways to improve password-based security is to utilize multi-factor authentication (MFA).

Reminder: When you are prompted to report at least two types of evidence to authenticate your identity during log-in, you're using MFA, which is also known as two-factor authentication (2FA). The **National Institute of Standards and Technology** (NIST) promotes this "additional layer of security" and offers this great example of how it works: "First and most typically, you'll type in your username and password. Then, as a second factor, you'll use an authenticator app, which will generate a one-time code that you enter on the next screen. Then you're logged in - that's it!"

Take a look at these password tips that **Adam Kehler, CISSP,** a principal consultant and healthcare practice lead with **Online Business Systems,** recommends for healthcare entities:

- **Length:** Longer passwords equal greater security - it's just that simple. "Increase length to 10 or 12 characters," he suggests.
- **Complexity:** An overly complicated password that must be changed weekly or monthly can be a headache and lead to password fails. "Eliminate requirements for complexity and scheduled change - only change if a password has been compromised" instructs Kehler.
- **Breach list:** It's never a great idea to reuse a password that's already created problems in the past. "Reject passwords that appear on a breached password list," he says.
- **Resets:** It's best not to overcomplicate the reset processes for users' passwords. "Make password resets easy by sending a temporary link to the user's backup email account," Kehler maintains.
- **Hints:** Hackers can easily investigate a user's background with just a username, so avoid using personal hints to remind about passwords. "Eliminate password hints; they actually decrease security," he warns.
- **Storage:** "Ensure passwords are stored using a strong, non-reversible hash like Bcrypt instead of SHA256," explains Kehler.
- **User-friendly practices:** "Increase usability with methods such as providing real-time feedback on password strength and ensuring systems are compatible with popular password safes," he says.

Resource: Check out NIST's MFA guidance at www.nist.gov/itl/tig/back-basics-multi-factor-authentication.