Health Information Compliance Alert

Cybersecurity: Know the Facts on Usernames and Passwords

Check out updated NIST guidelines for federal clarification.

Many practices take steps to circumvent unauthorized access by utilizing tools like antivirus software, firewalls, and more. But even with the strongest security measures in place, healthcare organizations continue to be vulnerable to cyber attacks. Plus, due to the sensitive nature of the patient data exposed, entities must be on top of these potential risks.

Context: The **Department of Health and Human Services Office for Civil Rights** (OCR) announced a small $100,000 settlement with **Medical Informatics Engineering, Inc.** (MIE), an Indiana-based software and EMR company. At the root of the HIPAA violation was a failure to assess risks that allowed cyber thugs to hack into its firm through a "compromised user ID and password," an OCR brief suggests. The end result was the disclosure of 3.5 million individuals' electronic protected health information (ePHI) (see story, p.41).

Review This Username Advice

The best usernames allow IT staff to identify individuals easily. In fact, usernames are often standard and don't allow for much differentiation by the individual employees.

"Usernames at work aren't usually up to the individual; they're set by the IT department and they usually follow a common standard such as 'first_initial.''last_name,' but you can take steps to keep your work username more secure by using it only for work," advises **Jen Stone, MSCIS, CISSP, QSA**, a security analyst with **Security Metrics** in Orem, Utah.

"Username formats should meet a corporate standard for consistency, but should not be considered confidential information," explains **Adam Kehler, CISSP**, principal consultant and healthcare practice lead with **Online Business Systems** agrees.

The format should essentially promote easy identification and allow IT to quickly assess who should or should not be accessing practice data. Moreover, if a data security issue does arise, IT staff can quickly identify the account involved and do damage control on the incident.

Tip: Don't mix work with pleasure. It's a good idea to use different usernames for your home accounts versus your work ones. Separating your work tech from your home tech not only protects patients, but it protects you, too.

Here's why: "If you use your work email as an account name, chances are good you'll be tempted to use your work password as well," warns Stone. "Then, when 'Flower Sparkle Games' is hacked, the hackers not only get access to your game, they also get access to your work account."

Create Stronger Password Controls With 4 Expert Tips

You may not put much thought into the creation of your work passwords, but you should. If your practice experiences a breach, one of the first things the feds will ask about is risk assessment - and weak password controls will be seen as ignoring potential risks.

Consider these four password must-dos that **Adam Kehler, CISSP**, a principal consultant and healthcare practice lead with **Online Business Systems,** suggests for users:

1. MFA: Put multi-factor authentication into use when sites allow it.

CPT® 2023 American Medical Association. All rights reserved.

2. Password safe: "Use a password safe that is compatible with all of your devices," he advises.

3. Arbitrary passwords: Make your passwords "random and unique" and add them to your password safe.

4. Outside-the-box hints: Some sites require hints, "use random words" instead of meaningful ones "and store those in the password safe," he says.

Set Reasonable But Strong Password Protocols

In recent years, password security has become a hot topic in healthcare as unauthorized access continues to be a thorn in the side of many covered entities (CEs) and their business associates (BAs). The HIPAA Security Rule points repeatedly to the importance of "policies and procedures" that protect the integrity of ePHI. And whether you're a CE operating a small practice in a rural zone or a multi-layered BA across several states, you must put risk analysis and password protection at the top of your HIPAA compliance planning.

"Passwords alone are by-and-large not a great way to authenticate individuals. Organizations should strongly consider implementing multi-factor authentication (MFA) for all remote access or privileged access to sensitive systems," Kehler says. "Implementing these controls can result in an incredible decrease of the number and severity of breaches."

Remember: The **National Institute of Standards and Technology** (NIST) updated its password guidance with recommendations for improving identity security. The new guidelines bemoan complicated composition rules for passwords because they create more problems. (see Health Information Compliance Alert, Vol. 19, No. 6).

"Research and the updated NIST SP 800-63B Digital Identification guidelines agree that most of what we know about password strength is incorrect," says Kehler. "Passwords change and complexity rules generally result in password reuse, writing down passwords, and creating predictable passwords such as 'Password123.'"

Tip: If your practice struggles with password management, you may want to consider using a password management tool. "In my experience, the best passwords come from a password manager," counsels Stone. "They can be long, complex, and unique without taxing your ability to remember all the passwords to all your accounts."

Stone adds, "More importantly, make sure two-factor authentication (2FA) is turned on for all your accounts. It might take a few more seconds for you to login, but the increased security is absolutely worth it!"

Resource: Read NIST's guidelines at https://pages.nist.gov/800-63-3/.

CPT® 2023 American Medical Association. All rights reserved.