Health Information Compliance Alert

Security: 5 Building Blocks to Construct a Secure Password Policy

Use these elements to keep your passwords -- and your patients' PHI -- out of sight

There is no such thing as an indestructible password. But with the right components, you can create a password policy that will ensure the privacy and security of all your confidential information. Here's some professional guidance to get you started.

1. Immediately change default codes.

Even the strongest password policy won't save you from a hacker sneaking into your system through a "back door" such as a default application or server password. This is usually the first line of attack.

Think of it this way: Hackers scan your systems for default codes much "like someone walks through a parking lot trying all the car doors until they find one that's unlocked," explains **Greg Young**, security officer for Mammoth Hospital in Mammoth Lakes, CA.

That means your first step to protecting your organization is to create unique passwords to replace the default ones before you walk away from the system.

2. Use all your tools.

The weakest passwords are short and usually contain dictionary words. You can combat this problem by defining exactly how your organization will create their passwords.

At a minimum, you should demand staffers use "a mixture of lower case, upper case, numbers and special characters like exclamation points or the @ symbol," says **Fred Langston**, principal consultant with VeriSign in Seattle.

Caution: You must balance ideal security against your users' ability to memorize long, complicated passwords without writing them down, Young warns. "A great password from a security point of view might be T2&38Zy#@s, but it's useless if no one can remember it," he notes.

Best approach: Ask each staff member to think of a slogan or phrase, like Visa's popular tagline, "It's everywhere you want to be." Then reduce the phrase to the first letters of each word and add a few capital letters: IeyWtB. Now you can replace a few letters with numbers and symbols. For example, you could replace I with 1, e with 3 and T with + to get your final result: 13yW+B - a tough password to crack.

Using a phrase or slogan along with your other rules will "give users something to remember in their heads so that they don't have to write anything down," Langston asserts.

However, if they must write something down, ask them to write the entire phrase rather than password itself, offers **Kelly Moore,** privacy and security officer for Daytona Beach, FL's Cogent Health Care. And instruct them to write their slogan "on paper and then stick it in their wallet so it leaves with them at the end of the day," she urges.

3. Enforce an expiration date.

Even the greatest passwords must be changed on a regular basis, experts agree. While the standard amount of time for requiring a new password is 90 days, you should "set your parameters based on what's reasonable for your systems and your company," Moore advises. "We're still debating between 90 and 120 days," she notes.

Though the length of time before passwords expire can differ, you want to be sure not to ask your users to change them too often or remember too many, Langston counsels. So while a high-sensitivity database may require new passwords every 45 days, that's probably too soon for regular security.

4. Don't recycle passwords.

Once your staffers find a really well built, strong password, they probably won't want to change it. But reusing passwords could lead to a security hole, cautions **Ali Pabrai,** CEO and co-founder of HIPAAAcademy.net.

Good idea: It's difficult to completely axe recycled passwords, but you could enforce a policy that forces users to construct new passwords until a certain amount of time has passed. For example, you may decide that your organization can reuse passwords after five expiration periods have lapsed, explains Langston.

5. Lock out repeated login mistakes.

One huge red flag in password security is multiple attempts to login without success. This is usually a sign that someone is trying to crack the password, Pabrai notes. Best practice: "Your system should lock accounts after someone misses logging in five times in a row," Langston says.

Tip: Instruct your users to contact your tech staff if they cannot remember their password, or if they find themselves locked out of the account. That way, you can maintain staffers' productivity and spot any trends -- such as a hacker systematically running through your users' accounts trying to get into your system.

The Bottom Line: Give your organization members a strong policy that outlines exactly how their passwords should be built. Tip: Remind staffers that you are available to help them construct a password if they are hesitant to make a choice.