COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 27, Number 35. October 08, 2018
Password Complexity Puts Hospitals At Risk; Single Sign-On Is An Option

By Nina Youngstrom

Unauthorized access to one employee's password could compromise a health care organization's network and data, yet traditional password security depends on employees remembering longer, more complex versions. Because passwords are the gateway to computers and mobile devices and often the target of phishing attacks, organizations are considering multifactor authentication and single sign-on solutions to protect sensitive information. They also may want to inform their patients they would never ask for passwords or credit card information by email.

"Passwords are universally a difficult thing for people to come up with. The goalpost always seems to change," says Alexander Laham, information security manager at Lawrence General Hospital in Massachusetts. Employees initially had to remember eight alphanumeric characters, then it was 10, and now it's up to 12 or 15. "We're trying to come up with a way to make passwords easier to use but maintain the security we require."

Password security is one of the top five security priorities for fiscal year 2019, he told his hospital's board of directors in late September. "I try to give them a snapshot of what we are concerned about in security. At any point in time, if someone were to ask them what the hospital is worried about, I want them to be prepared," Laham says. He provides the board with a strategic plan, which is an overarching description of what the security department will accomplish in the subsequent three years, and the tactical maneuvers for getting there.

Lawrence General Hospital is trying to balance the goals of reasonable passwords and hacker-resistant security (or somewhere in the neighborhood of that). It uses single sign-on as a way of logging into a computer. For example, end users (e.g., nurses) use their badges to sign into their computer, which recognizes who they are. "Instead of having to type in their password, there's a proximity card reader that identifies who they are and pulls their profile and logs into their account," he says. It's not a complete solution—the card reader isn't given to all employees because the technology and IT work behind it is expensive, and a lost badge would give the finder access to protected health information (PHI) and other data—but it's very useful for people who bounce from computer to computer in the course of their work, including clinicians, Laham says.

Single Sign-On Solves Some Problems

Single sign-on is similar to password managers in the sense of giving end users access to multiple accounts with one entry point. Mark Lanterman, chief technology officer at Computer Forensic Services in Minnetonka, Minnesota, recommends password managers, which are software applications that allow organizations to push out complex, unique passwords for every employee. They are automated and can be changed routinely. "At the push of a button, [the app] generates new passcodes," Lanterman says. Employees don't have to memorize them; they're stored securely on their computer or other device, such as a cell phone. But they will need one strong password to unlock the others. "I believe online accounts that can be accessed by anyone with a phone or computer require long, complicated passwords," he says. "Does your phone really need a 15-character password, since you have it in your pocket and it's under your physical control? Probably not."

Multifactor authentication also looks promising. It's a combination of something you know (e.g., a password); something you are (e.g., a fingerprint or iris scan); and something you have (e.g., a USB device, which is a security key that's unique to the user and allows access to his or her data). Google has not had any phishing attacks since its 85,000 employees were required to use passwords and USB devices in early 2017, according to , a cyber security blog. "Employees carry keys that validate who they are. It's great in theory, but in a health care setting, that's hard to use because you need speed," Laham notes. "Password security will always be a risk until we look at new technology like multifactor authentication."