COSMOS
Navigate the Compliance Universe

Compliance Today - June 2022
Password conundrum

By Jan Elezian, MS, RHIA, CHC, CHPS

Jan Elezian (jan.elezian@sunhawkconsulting.com) is a consultant and Director at SunHawk Consulting, LLC.

- linkedin.com/in/jan-elezian-30821011/


Jan Elezian

There's an app for just about everything these days. Online banking, games, email, services, shopping, and even accessing your health records require a password to enter. Each application asks you to supply a secret password that stops other people from entering without your permission. The Cybersecurity & Infrastructure Security Agency experts guide us to create a strong, complex password that is difficult for others (hackers) to guess.[1] Every application has rules for creating what it construes to be a strong and complex password. Some dictate at least eight characters but fewer than 12. Others ask for at least one capital letter, a number, and a symbol. Some have a combination of each. Added to the recommendation that passwords are unique, the user has the conundrum of remembering and storing potentially dozens of passwords.

Those who use, transmit, and store protected health information must follow the HIPAA password requirements, which require covered entities (CEs) to "develop and implement procedures for creating, changing, and safeguarding passwords."[2] Most CEs use passwords to protect individuals' health records from unauthorized disclosure. Yet, HIPAA is not specific on how passwords should be created, changed, and guarded. Thus, CEs and their business associates must develop their own password policies that comply with published Security Rule standards.

One recommendation is to follow the National Institute of Standards and Technology (NIST) security guidelines when creating internal password policies. Its latest guidance updates password best practices, summarized below:[3]

- Password length is more important than password complexity. Allow password field length of at least 64 characters.
- Don't enforce regular password resets. Only reset if there is evidence that a password has been compromised.
- Screen all new passwords against lists of commonly used and compromised passwords.
- Enable "Show password" while typing. The longer and more complex the entry text, the greater likelihood of user entry errors.
- Due to the greater likelihood of user entry errors, allow at least 10 failed password entries before account is locked out.
- Implement two-factor authentication to stop phishing attempts from succeeding.

Most experts believe that password management is not the strongest measure of security. Eliminating passwords altogether is proposed to be a better measure. Although there is a ways to go before passwords become obsolete, that day is coming. Biometric technology is becoming sophisticated and widely adopted.[4] For instance, the use of facial recognition and fingerprint readers is becoming commonplace. Those types of measures, the use of email authentication, and social media authentication may let us forget about remembering complicated passwords for good.

1 "Do Your Part. #BeCyberSmart: Creating a Password," National Cybersecurity Awareness Month, Cybersecurity and Infrastructure Security Agency, accessed April 8, 2022, https://bit.ly/3r7shrV.
2 "What are the HIPAA Password Requirements?" NetSec.News, March 18, 2021, https://www.netsec.news/hipaa-password-requirements/.
3 Paul A. Grassi et al.,*Digital Identity Guidelines: Authentication and Lifecycle Management*, NIST Special Publication 800-63B, updated March 2, 2020, http://pages.nist.gov/800-63-3/sp800-63b.html.
4 David Konetski, "It's the End of Passwords as We Know It," Dell Technologies blog, October 12, 2021, https://www.dell.com/en-us/blog/it-s-the-end-of-passwords-as-we-know-it/.