COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 10. October 05, 2023 OCR: Add Multi-Factor Authentication As HIPAA Security Best Practice

By Jane Anderson

The HHS Office for Civil Rights (OCR), noting that poor authentication practices have contributed to multiple high-profile cyberattacks and breaches, is urging HIPAA-covered organizations to review and improve their authentication practices.

In a recent newsletter, OCR said stronger authentication practices could impede or prevent many cyberattacks—particularly attacks that rely on the use of weak or stolen passwords.[1]

“Robust authentication serves as the first line of defense against malicious intrusions and attacks, yet a recent analysis of cyber breaches reported that 86% of attacks to access an organization’s Internet-facing systems (e.g., web servers, email servers) used stolen or compromised credentials,” OCR said.

OCR pointed out that in 2021, “a major food company that processes approximately 20% of the United States’ meat supply temporarily shut down several plants in response to a ransomware attack where the perpetrator gained initial access by compromising an old administrator account protected only by a ‘weak password.’”

In addition, a major fuel pipeline shut down in 2021 due to a ransomware attack that “started with a single stolen password linked to an old user profile,” OCR reported.

“Effective authentication ensures that only authorized individuals or entities are permitted access to an organization’s information systems, resources, and data,” OCR said. “HIPAA regulated entities are required to implement authentication solutions of sufficient strength to ensure the confidentiality, integrity, and availability of their ePHI [electronic protected health information].”

Authentication Defined

Authentication corroborates that a person is the person they claim to be, OCR said. This corroboration of a person’s identity “is the prerequisite to allow access to resources (e.g., computer systems, data) to only those authorized for such access,” OCR said.

The “classic” style of authentication is presenting credentials, which usually consist of an identifier (such as a login) and one or more authentication factors, OCR said. Traditionally, authentication has been based on three factors:

- “something you know (e.g., password or personal identification number (PIN))
- “something you have (e.g., smart ID card or security token)
- “something you are (e.g., fingerprint, facial recognition or other biometric data)”

Single-factor authentication needs one of those factors—typically, just a password (something you know), OCR said. To enable multi-factor authentication, two or more unique factors must be used, the agency said.

Importantly, OCR said “authentication that requires a user to prevent multiple instances of the same factor is not multi-factor authentication. For example, an authentication process requiring a password and PIN is not multi-factor authentication because both factors are ‘something you know.’”