THOMSON REUTERS®

OCR Cybersecurity Newsletter Addresses HIPAA and Cybersecurity Authentication

EBIA Weekly (July 20, 2023)

June 2023 OCR Cybersecurity Newsletter: HIPAA and Cybersecurity Authentication (June 29, 2023)

Available at https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-june-2023/index.html

HHS's Office of Civil Rights (OCR) has released its latest cybersecurity newsletter, highlighting the importance of having strong authentication processes to "lock the door" in the cyber world and prevent cyberattacks that may result in unauthorized access to electronic protected health information (ePHI). According to OCR, weak and non-existent authentication processes "leave your digital door open," and can lead to increased cyberattacks that use weak or stolen passwords. The newsletter explains the different methods of authentication, making the case that stronger multifactor authentication processes make it more difficult for attackers to gain unauthorized access to information systems. Single factor authentication typically requires an identifier (e.g., a username) and one factor (e.g., a password, token or fingerprint). Multifactor authentication requires two or more distinct factors and is designed to make it more difficult to gain access.

The newsletter points covered entities to recommendations from the Cybersecurity and Infrastructure Security Agency (CISA) that phishing-resistant multifactor authentication be implemented on internet facing systems (e.g., email or remote desktop). It notes that while the HIPAA Security Rule does not define specific authentication solutions, multifactor authentication may sometimes be necessary to reduce risks—for example, with respect to remote access to ePHI. OCR stresses that HIPAA covered entities have an ongoing obligation to assess whether stronger authentication systems are necessary. A risk analysis of the location of ePHI should consider whether multifactor authentication solutions are necessary to improve the security of ePHI and protect systems from cyberattacks.

EBIA Comment: The newsletter is a reminder of the ongoing need to implement authentication solutions that are sufficient to protect ePHI. According to OCR, a recent analysis of cyber breaches reported that 86% of attacks to access an organization's internet-facing systems used stolen or compromised credentials. Additionally, an HHS task group encourages the use of multifactor authentication for remote access to systems and email as a best practice. OCR reminds covered entities that a thorough risk assessment should periodically consider whether the security of ePHI requires stronger phishing-resistant multifactor authentication. For more information, see EBIA's HIPAA Portability, Privacy & Security manual at Sections XXX.D ("Technical Safeguards"), XXV.H, ("Breach Planning and Response"), XXIX.E ("Developing Your Security Program") and XXX.B.6 ("Standard: Security Incident Procedures").

Contributing Editors: EBIA Staff.