Published on *The National Law Review* https://natlawreview.com

HHS-OCR Explains How HIPAA Security Rule Requirements Protect Against Cyberattacks

Article By:

Mary Elizabeth “Lizzie” Ford

Stacy L. Cook

On Oct. 30, in honor of National Cybersecurity Awareness Month, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) released a video regarding how the HIPAA Security Rule can help protect healthcare entities against cyberattacks. The video, which featured Nicholas Heesters, OCR's senior advisor for cybersecurity, covers several topics. Below are the highlights:

1. **Changes in HIPAA breach trends.** According to Heesters, in 2009, the most common cause of a large HIPAA breach (impacting 500 or more individuals) was device theft. In 2023, the most common cause of a large HIPAA breach is a remote cyberattack.
2. **Practical ways to stop a cyberattack**. Heesters reiterated the importance of following the administrative, physical, and technical safeguards of the HIPAA Security Rule. He also explained the importance of developing strong device passwords and requiring employee phishing training. Heester noted that cyberattacks are most likely to occur via a phishing

scheme against non-managerial employees that allows the attacker to break into the system.

3. **Resources**. Heesters encouraged viewers to review OCR's resources and guidance regarding the HIPAA Security Rule, including a June 2023 newsletter on multifactor authentication .

HIPAA covered entities and business associates are required to implement various safeguards to protect protected health information (PHI), including the safeguards that protect against cyberattacks.

National Law Review, Volume XIII, Number 313