OCR Cybersecurity Newsletter Addresses Social Engineering

EBIA Weekly (November 7, 2024)

October 2024 OCR Cybersecurity Newsletter: Social Engineering: Searching for Your Weakest Link

Available at ***https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-october-2024/index.html***

HHS's Office for Civil Rights (OCR) has released its latest cybersecurity newsletter, highlighting that HIPAA covered entities and business associates are at risk for social engineering cyber threats. Social engineering is when an attacker uses emails, texts, calls, or videos and tries to manipulate someone to open links or documents and provide information that can be used to compromise systems or networks. Covered entities and business associates are invited to conduct risk assessments that review emerging social engineering threats, and deploy safeguards such as anti-phishing technologies, scanning web links or attachments, and using machine learning or behavioral analysis to detect and prevent potential threats. The newsletter points out that individuals are often the "weakest link" in exposing covered entities and business associates to social engineering threats and outlines how HIPAA covered entities, business associates, and individuals can defend against them:

- *Phishing and Smishing.* Phishing occurs when an attacker sends an email that appears to be from a legitimate source that manipulates an individual to provide sensitive information or download malicious software that compromises systems. An example of phishing is an email from what appears to be the HR department asking the employee to click a link and provide a password. Smishing occurs when Short Message Service (SMS) messaging (i.e., texts) tricks someone into sharing their sensitive information through clicking a link, downloading software, or making a call. An example of smishing is when a message appears to come from a bank asking to confirm a large withdrawal by making a call or clicking a link to reset a password. To avoid smishing or phishing exposure, the newsletter suggests training to show employees how to vet unexpected email that may not be legitimate and verify phone numbers before providing any usernames, passwords, or personally identifiable information.
- *Baiting.* Baiting involves luring individuals with the promise of something valuable such as winning a prize, enticing them to click on a link that then installs malicious software on their computer or phone. Sometimes baiting involves leaving devices in public places (such as a lobby) that can be used to breach information systems if plugged in. To avoid baiting, OCR recommends being skeptical of offers that require providing credentials or clicking on unverified links and avoiding unattended devices.
- *Deepfakes.* A deepfake occurs when someone believes they are communicating (e.g., through video, photo, audio) with a trustworthy source which is faked through artificial intelligence (AI) technology, using AI cloning to convince the individual to provide access to sensitive data such as protected health information (PHI). To avoid deepfake manipulation, some key signs to look for include inconsistent eye blinking, lack of facial features with clear definition, unnatural skin discoloration, a person's mouth not synchronizing to what they are saying, and abnormal boundaries between hair and background. Another way to determine if it is a deepfake is to disconnect the call or text and confirm the number is verified.

EBIA Comment: The newsletter reminds covered entities and business associates to implement a HIPAA security awareness and training program that includes testing workforce member knowledge. Links are provided to several resources related to social engineering. The newsletter comes during the same month that OCR updated question 11 of its **FAQs** on the Change Healthcare cybersecurity incident to include that approximately 100 million individual breach notices have been sent. Together, these actions highlight that OCR is focusing on enforcement of cybersecurity breaches, often citing covered entities and business associates for failure to have updated risk assessments, policies and procedures, and training. For more information, see EBIA's HIPAA Portability, Privacy & Security manual at Sections XX ("Enforcement of Privacy, Security, and EDI Rules"), XXIII ("How the Privacy and Security Rules Affect Group Health Plans and Plan Sponsors"), XXIV ("Business Associate Contracts"), and XXV ("Breach Notification for Unsecured PHI").

Contributing Editors: EBIA Staff.