HHS Phishing Attack Investigation Results in $600,000 Payment to Settle Potential HIPAA Violations

EBIA Weekly (May 8, 2025)

PIH Health, Inc. Resolution Agreement and Corrective Action Plan (Jan. 28, 2025); HHS Press Release (Apr. 23, 2025)

Resolution Agreement

Press Release

HHS's Office for Civil Rights (OCR) has announced a settlement with a HIPAA covered entity concerning potential violations of HIPAA's privacy, security, and breach notification rules. OCR initiated an investigation after receiving a breach report from the covered entity concerning a phishing attack that affected 45 employees' email accounts, leading to a data breach of over 189,000 individuals' electronic PHI (ePHI). The information exposed included names, addresses, birth dates, driver's license numbers, Social Security numbers, medical diagnoses, lab results, medications, treatment and claim details, and financial information.

OCR found, among other things, that the covered entity failed to conduct a compliant risk analysis, implement security measures to reduce the risks and vulnerabilities to ePHI, and provide timely breach notifications to individuals, HHS, and the media. The investigation resulted in a settlement payment of $600,000 and a corrective action plan that requires the covered entity to conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to ePHI; develop and implement a written risk management plan to mitigate the risks and vulnerabilities identified in the risk analysis; develop, maintain, and revise its written policies and procedures regarding privacy and security as needed to comply with HIPAA; and provide workforce training on its HIPAA policies and procedures.

EBIA Comment: This settlement highlights the critical importance of adhering to HIPAA's rules, including conducting thorough risk analyses, implementing robust security measures, and ensuring timely notifications of data breaches. It is also a reminder that ongoing vigilance is required to protect ePHI in an increasingly digital health care environment. The press release notes that "hacking is one of the most common types of large breaches reported to [HHS's Office for Civil Rights] every year." This and other resolution agreements demonstrate that HHS continues to focus on ransomware and risk analysis initiatives. Covered entities are advised to take these steps to prevent cyber threats: (1) identify where ePHI is stored and how it moves through the organization; (2) integrate risk analysis and management plans into business processes; (3) ensure audit controls are in place to monitor system activity; (4) regularly review system activity; (5) use authentication to ensure only authorized users access ePHI; (6) encrypt ePHI during transmission and storage to prevent unauthorized access; (7) learn from past incidents to improve security management; and (8) provide regular, job-specific HIPAA training to staff. Covered entities can review an HHS cybersecurity newsletter on social engineering for recommendations on avoiding phishing vulnerability risks like the incident in this investigation. 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"), XXV ("Breach Notification for Unsecured PHI"), XXIX ("Security Requirements: General Concepts"), and XXX ("Core Security Requirements").

Contributing Editors: EBIA Staff.