MINTZ

Gone Phishin': Hack Leads to HIPAA Settlement

April 14, 2017 | Blog | By

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

While your business may indeed be a "victim" when hit by a phishing attack, your enterprise can also be responsible for violations of law associated with the incident. Earlier this week, the **HHS Office for Civil Rights** ("OCR") announced **a $400,000 settlement** with Metro Community Provider Network ("MCPN") related to a 2012 HIPAA breach caused by a phishing scam. The phishing scam, carried out by accessing MCPN employees' email accounts, gave a hacker access to the electronic protected health information ("ePHI") of 3,200 individuals. In investigating the breach, OCR determined that, **prior to the breach, MCPN had not conducted a security risk analysis (a requirement under HIPAA). Further, OCR found that even after MCPN conducted a risk analysis, its analysis was insufficient to meet the requirements of the HIPAA Security Rule.**

In addition to the $400,000 fine, MCPN agreed to a corrective action plan with OCR. That plan requires MCPN to conduct a comprehensive risk analysis and to submit a written report on the risk analysis to OCR. Additionally, MCPN will be required to develop an organization-wide risk management plan, to review and revise its Security Rule policies and procedures, to review and revise its Security Rule training materials, and to report to OCR any instance of a workforce member failing to comply with its Security Rule policies and procedures.

The MCPH settlement underscores the **importance of risk analyses and workforce training** to avoid phishing scams. Additionally, it is crucial that entities regulated by HIPAA conduct an enterprise-wide HIPAA risk analysis, update that analysis to address new threats, and implement policies and training based on identified risks. Failure to comply with these essential HIPAA requirements can turn a relatively routine breach investigation into a $400,000 settlement.

A copy of the MCPN resolution agreement and corrective action plan is available **here**. OCR's press release on the settlement is available **here**. General Security Rule guidance from OCR is available **here**.

Authors