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

Malicious Malware Brings On a Major HIPAA Headache

Article By:

John E. Wyand

Sarah H. Stec

The United States Department of Health and Human Services (HHS) recently entered into a $750,000 resolution agreement with the University of Washington (UW) following an investigation. The investigation was prompted by UW reporting a breach of about 90,000 people's personal health information (PHI) after an employee unknowingly downloaded malicious malware from an email attachment.

Similar to other enforcement actions, HHS is heavily involved in UW's corrections and corrective actions. UW must not only conduct a risk analysis that addresses cybersecurity risks to ePHI, reviewable by HHS before it can be fully accepted, but also create a new risk management plan that addresses the risks found in the risk analysis. UW must also review everything on an annual basis and update HHS accordingly.

In HHS' press release announcing the resolution agreement, OCR Director Jocelyn Samuels stated, "All too often we see covered entities with a limited risk analysis that focuses on a specific system . . . [a]n effective risk analysis is one that is comprehensive in scope and is conducted across the organization . . . ." It's clear that no organization is too big or complex to ignore its HIPAA compliance responsibilities. Having robust compliance procedures and policies, and reviewing them to ensure that they work as they are supposed to, is key for companies of all sizes to avoid expensive enforcement actions.

© Copyright 2024 Squire Patton Boggs (US) LLP

National Law Review, Volumess V, Number 352

Source URL:https://natlawreview.com/article/malicious-malware-brings-major-hipaa-headache