NOVEMBER 2023

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

OCR Faults Business's Data Security Practices After Ransomware Attack

The U.S. Department of Health and Human Services, Office for Civil Rights (OCR) recently announced its first settlement agreement related to a ransomware attack. But it was not the ransomware that triggered OCR's enforcement action—it was likely the regulated entity's failure to detect (and thus report) the breach for nearly two years.

While ransomware continues to be a scourge on hospitals (OCR notes ransomware attacks have increased 278% over four years), OCR's public statements suggest it will pursue settlements or enforcement actions in connection with such attacks only where there are aggravating factors. These aggravating factors will likely include (1) the failure to identify and address actual security risks a business may face; (2) the failure to conduct meaningful vulnerability assessments; and (3) the failure to implement measures to detect security incidents. Below are practical tips organizations should consider to mitigate the risk of drawing OCR's ire in connection with a ransomware attack.

Practical Tips

1. **Identify Organization-Specific Vulnerabilities.** Regulated entities should review their policies and tools to ensure they identify and address specific vulnerabilities affecting electronic protected health information (ePHI). To do this, organizations should maintain an inventory of all of their facilities, electronic equipment, data systems, and applications that contain or store ePHI. Key stakeholders should participate in this process to ensure that the current organizational risks are addressed. This inventory should then be incorporated in an organization's risk analysis.

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Lindsey Knapton
Associate
303.285.5534
lknapton@shb.com

2. **Develop Tailored Risk Analysis.** Covered entities should develop (and regularly update) risk assessments and related risk-management plans tailored to the specific risks they face for securing ePHI. Risk-management analysis should consider network segmentation, network infrastructure, vulnerability scanning, logging and alerts, and patch management. In addition, these plans should be updated when new technologies or business operations are adopted.
3. **Monitor Network Activity.** To quickly detect security incidents, organizations should implement audit controls to promptly monitor, review, and analyze information system activity captured in audit logs, access reports, and security incident tracking reports.

Background

A business associate that provides medical billing and payor credentialing notified OCR of a data breach on April 22, 2019. The organization explained that an intruder first accessed its system in April 2017. But the intrusion went undetected for nearly two years; the organization only learned of the breach in December 2018 when a threat actor deployed the ransomware, which encrypted the organization's files. The breach impacted 206,695 patients' ePHI.

OCR's Investigation and Settlement

OCR opened an investigation in April 2019, shortly after receiving notification. OCR identified several shortcomings concerning the organization's compliance with HIPAA's Privacy and Security Rules, including the failure to:

- monitor activity on information systems;
- analyze potential risks and vulnerabilities to ePHI across the organization; and
- implement policies and procedures as required by HIPAA's Security Rule.

More than four years after it opened an investigation, OCR announced a settlement with the organization. The settlement required a $100,000 payment to OCR and implementation of a Corrective Action Plan (which will remain in effect for the next three years). In the press release concerning the settlement, OCR emphasized that the organization failed to adequately protect patient data and advised regulated entities to "take steps to identify and address cybersecurity vulnerabilities along with proactively and regularly review[ing] risks, records, and updat[ing] policies."

Josh Hansen
Associate
303.285.5306
jahansen@shb.com

Al Saikali
Chair, Privacy and Data Security Practice
305.358.5171
asaikali@shb.com

The choice of a lawyer is an important decision and should not be based solely upon advertisements.