Recent Enforcement Actions Demonstrate That Cyberattacks Present Huge HIPAA Liability for Medical Practices

Ransomware and hacking continue to be primary cyberthreats in health care. Since 2018, the US Department of Health and Human Services has seen a 264 percent increase in reported large ransomware breaches of electronic health information. When providers experience a ransomware attack, any breach of electronic protected health information (ePHI) must be reported to the HHS Office of Civil Rights (OCR) under the HIPAA Breach Notification Rule. OCR follows up these reports with investigations and, if necessary, enforcement actions. In October 2023, OCR settled its first ransomware case, imposing a $100,000 fine and corrective action plan on a vendor that provided services to health care entities as a HIPAA business associate. OCR has now concluded seven enforcement actions against providers, resulting in the imposition of substantial civil penalties. In the last four months alone, OCR has announced four settlement agreements with providers who failed to secure their systems against cyberattacks. This increased activity highlights the need for providers to be especially vigilant in protecting against cyberthreats.

On September 26, 2024, OCR announced a settlement with Cascade Eye and Skin Centers, a Washington-based health care provider. OCR received a complaint in 2017 and, upon investigation, learned that 291,000 patient files had been impacted by a ransomware attack. OCR found multiple potential violations of the HIPAA Security Rule, including the failure to conduct a compliant risk analysis to determine potential risks and vulnerabilities to ePHI and failure to adequately monitor its health information systems to protect against cyberattacks. The resolution agreement requires Cascade to pay $250,000 to OCR and enter into a corrective action plan that obligates Cascade to implement various controls and procedures, all of which must be reviewed and approved by HHS.

On October 3, 2024, OCR imposed a $240,000 civil penalty against Providence Medical Institute (PMI), a not-for-profit physician services organization in southern California with 275 providers across 35 medical offices. OCR received a report in April 2018 that PMI's systems were compromised by a series of ransomware attacks affecting approximately 85,000 individuals. The breach occurred at an orthopedic practice that PMI acquired and intended to fully integrate. Before integration occurred, a ransomware group encrypted the group's files after an employee responded to a phishing email and disclosed their credentials. OCR's investigation revealed that the provider's servers were encrypted with ransomware three separate times. Although PMI was able to restore systems from backup tapes within a few days. The files continued to be attacked by the threat actor, which had retained access to the data after it was restored from backups and used administrator credentials it obtained. Among the failures identified, there was no business associate agreement in place with PMI's data management vendor.

On October 31, 2024, OCR announced a whopping $500,000 civil penalty against Plastic Surgery Associates of South Dakota (PSA). PSA reported that that nine workstations and two servers were infected with ransomware affecting the ePHI of 10,229 individuals. The hackers obtained network credentials to PSA's remote desktop protocol through "brute force attack" (i.e., systematically using trial and error to guess passwords, login information, encryption keys, etc.). After discovering the breach, PSA was unable to restore the affected servers from backup. It

made two bitcoin ransom payments totaling over $27,000 in exchange for decryption keys from the hackers to regain access to its patients' ePHI.

Also on October 31, 2024, OCR announced its first ransomware enforcement action under its new Risk Analysis Initiative. A risk analysis is a required provision of the HIPAA Security Rule[i] for effective cybersecurity. The Risk Analysis Initiative was created by OCR to focus on compliance with this rule. Bryan County Ambulance Authority (BCAA), a provider of emergency medical services in Oklahoma, settled for $90,000 resulting from a 2022 ransomware incident that encrypted the files of 14,273 patients. OCR's investigation determined that BCAA had never conducted a risk analysis to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI, and the seriousness of the violation warranted a financial penalty.

These recent settlements illustrate that OCR is now vigorously investigating breach reports relating to cyberattacks and punishing providers when a ransomware attack is the result of an entity's failure to comply with HIPAA. Investigations conducted by OCR can lead to costly settlements and years of OCR oversight of a HIPAA-covered entity's compliance efforts. Providers must proactively safeguard patient data and conduct accurate and thorough risk analyses to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Providers can mitigate the likelihood of a substantial civil penalty by taking the following actions:

- Implement a risk management plan to address and mitigate security risks and vulnerabilities identified in their risk analysis.
- Develop a written process to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
- Develop policies and procedures for responding to an emergency or other occurrence that damages systems that contain ePHI.
- Develop written procedures to assign a unique name and/or number for identifying and tracking user identity in systems that contain ePHI.
- Review and revise as necessary written policies and procedures to comply with the HIPAA Privacy and Security Rules.
- Review all vendor and contractor relationships to ensure business associate agreements are in place as appropriate and address breach/security incident obligations.
- Ensure audit controls are in place to record and examine information system activity.
- Implement regular review of information system activity.
- Utilize multifactor authentication to ensure only authorized users are accessing ePHI.
- Encrypt ePHI to guard against unauthorized access to ePHI.
- Provide training specific to the organization and job responsibilities and on regular basis; reinforce workforce members' critical role in protecting privacy and security.

If you have any questions regarding the content of this article, please contact Fran Ciardullo, special counsel, at fciardullo@barclaydamon.com, or another member of Barclay Damon's Health & Human Services Providers Team.

AUTHOR'S BIOGRAPHY

Fran Ciardullo

As special counsel at Barclay Damon LLP, Fran concentrates her legal practice on health care and risk-management issues. She counsels physicians, physician groups, dentists, hospitals and health systems, nursing homes, and other health care providers on matters involving professional misconduct, professional liability, medical-staff issues, scope of practice, mandated reporting, peer review, and regulatory compliance. Fran also handles consent for treatment and surrogate decision making, patient care, EMTALA, and health-information privacy issues.

A former Town of Schroeppel town justice, Fran is also trained in alternative dispute resolution and has mediated and arbitrated a variety of civil actions and disputes. She routinely publishes industry articles and presents educational programs on legal matters to hospitals, medical and dental practices, and trade associations.

---

[i] *See* 45 C.F.R. § 164.308(a)(1)(ii)(A).