HHS Ransomware Cybersecurity Investigation Results in $250,000 Settlement

EBIA Weekly (October 3, 2024)

Resolution Agreement: Cascade Eye and Skin Centers (June 17, 2024); HHS Press Release (Sept. 26, 2024)

Resolution Agreement

Press Release

HHS's Office for Civil Rights (OCR) has announced a ransomware attack settlement with a health care provider (a covered entity under HIPAA) involving approximately 291,000 files containing ePHI. In May 2017, OCR received information indicating that the covered entity had experienced a ransomware attack, and that files containing ePHI were held at ransom. OCR's investigation revealed that the covered entity had engaged in multiple potential violations of HIPAA's security rule, including failures to conduct a compliant risk analysis and to sufficiently monitor its health information systems' activity to protect against a cyberattack.

The resolution agreement requires a $250,000 settlement payment and compliance with a corrective action plan (CAP) that OCR will monitor for two years. Under the CAP, the covered entity must, among other things: (1) conduct an accurate and thorough risk analysis of the potential security risks and vulnerabilities to ePHI that incorporates an inventory of all electronic equipment, data systems, off-site data storage facilities, and applications that contain or store ePHI; (2) develop and implement a risk management plan that addresses and mitigates any security risks outlined in the risk analysis; (3) develop and implement a written process to regularly review records of information system activity (i.e. logs, access reports, and security incident tracking reports); (4) develop and implement a contingency plan for responding to an emergency or occurrence that damages systems that contain ePHI; (5) develop written policies and procedures to assign a unique name/number for identifying and tracking user identity in systems containing ePHI; and (6) review, revise, and distribute to workforce members and business associates written HIPAA policies and procedures that meet the minimum content requirements outlined in the CAP and have been approved by HHS.

EBIA Comment: The press release states that OCR has seen a 264% increase in large ransomware breaches since 2018. OCR recommends that covered entities and business associates take steps to mitigate or prevent cyber-threats, including the following: (1) review business associate agreements to ensure that they address breach/security incident obligations; (2) integrate risk analysis and risk management plans into business processes; (3) ensure audit controls are in place (and regularly reviewed) to record and examine information system activity; (4) utilize multi-factor authentication to ensure that only authorized users can access ePHI; (5) incorporate lessons learned from incidents into security management processes; and (6) provide training on a regular basis. HHS has previously provided ransomware guidance to HIPAA covered entities and business associates, including a detailed fact sheet in 2016 and a cybersecurity newsletter in 2019. This is OCR's fourth ransomware settlement,

and covered entities are advised to review the agency's guidance and recommendations to ensure HIPAA compliance. For more information, see EBIA's HIPAA Portability, Privacy & Security manual at Sections XX.D ("Resolution Agreements"), XXVIII.H ("Policies and Procedures"), and XXX.D ("Technical Safeguards").

Contributing Editors: EBIA Staff.