PUBLICATION

The Office for Civil Rights Recently Settled Two Ransomware Related Investigations

Authors: Alisa L. Chestler, Layna S. Cook Rush
October 10, 2024

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) recently settled two ransomware cases with covered entities. These cases signal the government's growing concern with health care organizations' ability to plan for and potentially remediate vulnerabilities prior to any third-party threat actor attempting to compromise a system.

In early October, OCR settled its investigation and case with a health care provider in Washington state, Cascade Eye and Skin Centers, P.C., (Cascade) for $250,000 following a ransomware attack that exposed 291,000 files containing electronic protected health information (ePHI). Cascade is also required to implement an extensive corrective action plan with two years of ongoing monitoring. The Cascade settlement is OCR's fourth settlement involving a ransomware attack. In its announcement, OCR noted that it has seen a 264 percent increase in large ransomware breaches since 2018.

The Cascade case began on May 26, 2017, when Cascade filed a report with OCR. In the report to OCR, Cascade, which has several locations in Washington state, reported that it was the victim of a ransomware attack that had occurred in March 2017. OCR's investigation indicated potential violations of the HIPAA Security Rule including the requirement to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI and the requirement to implement procedures to regularly review records of information system activity.

Per the Settlement Agreement, in addition to the fine, Cascade Eye and Skin Centers is required to implement a corrective action plan that includes the following actions:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;
- Implement a risk management plan to address and mitigate security risks and vulnerabilities identified in their risk analysis;
- Developing a written process to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports;
- Developing policies and procedures for responding to an emergency or other occurrence that damages systems that contain ePHI;
- Developing written procedures to assign a unique name and/or number for identifying and tracking user identity in its systems that contain ePHI; and
- Reviewing and revising, if necessary, written policies and procedures to comply with the HIPAA Privacy and Security Rules

The resolution agreement and corrective action plan may be found here.

OCR announced its fifth settlement with a covered entity regarding a ransomware attack on October 8, 2024. Providence Medical Institute (Providence) in southern California was assessed a $240,000 penalty following OCR's investigation into the incident. According to its website, Providence is a non-profit physician services

organization with 275 providers across 35 medical offices. The Providence breach stems from its 2016 acquisition of a provider group. In July 2016, Providence acquired the Center for Orthopaedic Specialists (COS). Prior to July 2016, COS operated as an independent physician practice with its own IT network that had been managed and supported by an outsourced IT vendor. After Providence acquired COS, it initiated a two-year transition plan with the end goal of having COS utilize Providence's IT environment. The outsourced vendor remained COS's IT vendor while COS transitioned to Providence's network. COS's integration into Providence's infrastructure was not in place at the time of the attack.

OCR reported that Providence filed a breach notice in April of 2018, reporting that its systems were impacted by a series of ransomware attacks that affected the ePHI of 85,000 individuals between February and March of 2018. OCR learned through its investigation that servers containing ePHI were encrypted with ransomware three times. OCR found two potential violations of the HIPAA Security Rule, including failure to have a business associate agreement with a vendor that accessed ePHI, and failure to implement policies and procedures to allow only authorized persons or software programs to use its ePHI. OCR also found in its Proposed Determination that COS "utilized unsupported and obsolete operating systems to host its ePHI data; COS did not have a demilitarized zone (DMZ) network enabled or configured to separate its private network from the public internet and untrusted networks; COS's firewall was not properly configured to monitor and track access or changes to its network; and COS had Remote Desktop Protocols (RDPs) enabled which allowed insecure remote access to COS workstations from external sources. The assessment also found that at the time of the attacks, COS workforce members were sharing generic credentials with administrator access to log into COS's workstations, which allowed all users logging into COS's workstations to have unrestricted administrator access. The evidence collected during OCR's investigation indicates that the ePHI was accessible and viewable to the attackers because encryption was not deployed on COS's servers or workstations prior to the attacks."

The Notice of Proposed and Final Determinations for the Providence Medical Institute are available here.

In the announcements regarding these settlements, covered entities that are subject to the HIPAA Security Rule are urged to strengthen their cybersecurity protocols by reviewing vendor agreements, conducting regular risk assessments, enforcing audit controls, utilizing multifactor authentication, and encrypting ePHI. Regular training for staff and incorporating lessons learned from past incidents are also recommended to enhance overall security.

OCR settled its first ransomware case on October 31, 2023, imposing a $100,000 fine and corrective action plan on a vendor that provided services to health care entities as a HIPAA business associate. The fact that there have been four more settlements related to ransomware attacks in less than a year demonstrates that, while OCR had previously focused on education in the event of a ransomware attack, it is now more rigorously investigating these incidents and imposing liability when a ransomware attack is the result of an entity's failure to comply with HIPAA. This recent enforcement trend underscores the need for health care entities to proactively safeguard patient data to comply with the HIPAA Security Rule requirements and mitigate the risks of cyberattacks. For more information on this topic, please contact Layna Cook Rush, CIPP/US, CIPP/C, Alisa L. Chestler, CIPP/US, QTE, or your primary Baker Donelson attorney.