HIPAA Enforcement Action Against Employer-Sponsored Health Plan for Ransomware Attack

May 5, 2026

PRACTICES Employee Benefits and Executive Compensation

On April 23, 2026, the HHS's Office for Civil Rights ("***OCR***") announced a settlement with a self-funded employer-sponsored group health plan (the "***Plan***") following a ransomware attack that resulted in a breach of electronic protected health information ("***PHI***"). Under the settlement, the Plan agreed to pay $245,000 to OCR and to implement a two-year corrective action plan. While OCR routinely enters into settlement agreements with regulated entities, actions directly targeting employer-sponsored group health plans remain relatively rare, making this case noteworthy for plan sponsors.

In its investigation of the breach, OCR found that the Plan had failed to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its PHI, as required under the HIPAA rules. Although the breach was caused by a bad actor, the Plan did not have sufficient safeguards in place to protect the PHI.

This settlement serves as an important reminder for employers that sponsor self-funded group health plans. HIPAA security rules apply directly to the employer and require coordination with the employer's information security team. For example, HIPAA requires plans to conduct a risk analysis identifying where PHI may be located within the employer and to develop a risk management plan to address risks and vulnerabilities. This is separate from any HIPAA compliance actions performed by service providers to ensure the service providers are protecting PHI. The HIPAA security rules are also in addition to the HIPAA privacy rules, with which the employer's benefits team may be more familiar.

The OCR Settlement and Corrective Action Plan can be found here.