Articles + Publications | August 4, 2026

OCR Announces Notable HIPAA Enforcement Actions Against Self-Funded Group Health Plans Following Ransomware Breaches

WRITTEN BY

Brent T. Hoard | Emily D. Zimmer | Lydia Parker | Laura L. Ferguson | Emma E. Trivax

KEY POINTS

- OCR reached two 2026 settlements — totaling $695,000 — with self-funded group health plans following ransomware breaches, marking a notable expansion of direct HIPAA enforcement against self-funded health plans.
- Both plans were cited for failing to conduct an accurate and thorough risk analysis to identify vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) stored on plan sponsor systems.
- Self-funded group health plans are HIPAA-covered entities with independent compliance obligations that are separate from those of their plan sponsors, third-party administrators, and business associates.
- Plan sponsors should conduct a plan-specific HIPAA risk analysis that explicitly evaluates ePHI data flows and any connections between the plan's systems and the employer's corporate IT environment.
- OCR corrective action plans in both cases require comprehensive risk analyses, policy updates, workforce training, and periodic compliance reporting — requirements plan sponsors should proactively implement.

The U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) recently announced two separate settlements with self-funded employee group health plans, one sponsored by an energy provider and another sponsored by a national retailer (each, a Plan). The resolutions are notable as the first and second direct HIPAA enforcement actions against self-funded employer-sponsored group health plans, which are "covered entities" for HIPAA purposes.

APRIL 2026 ENFORCEMENT ACTION

Several years prior to the settlement, the Plan experienced a ransomware attack in which an unauthorized actor deployed ransomware on the plan sponsor's systems and exfiltrated personally identifiable information, some of which included electronic protected health information (ePHI). The Plan reported the breach to the OCR, and the OCR's subsequent investigation identified non-compliance by the Plan with HIPAA. In the enforcement action, the OCR specifically noted that the Plan failed to conduct an accurate and thorough risk analysis to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of Plan ePHI on the plan sponsor's systems. The Plan agreed to pay $245,000 and implement a monitored two-year Corrective Action Plan (CAP). The CAP requires the Plan to come into compliance with HIPAA by undertaking these requirements: conduct a comprehensive risk analysis for ePHI, develop and implement a risk management plan, update policies and procedures, and provide workforce training. The CAP requires the OCR's approval of the risk management plan

and revised policies, and the Plan must submit periodic reports to OCR with documentation proving and attesting to compliance with HIPAA.

JUNE 2026 ENFORCEMENT ACTION

This settlement arose after the Plan filed a breach report with the OCR detailing the Plan's discovery of an unauthorized actor that accessed the plan sponsor's network and deployed ransomware, encrypting data on the plan sponsor's systems (including servers storing the Plan's ePHI) and demanding a ransom. Upon investigation, the OCR found that the Plan failed to conduct an accurate and thorough risk analysis to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of Plan ePHI, and failed to implement reasonable and appropriate policies and procedures to comply with the HIPAA Privacy, Security, and Breach Notification Rules. The Plan agreed to pay $450,000 and implement a monitored two-year CAP. The CAP requires the Plan to conduct a comprehensive risk analysis for ePHI, review and revise (as needed) its HIPAA Privacy, Security, and Breach Notification Rule policies and procedures, provide workforce training, and submit periodic reports to the OCR.

KEY TAKEAWAYS FROM THE ENFORCEMENT ACTIONS:

- Self-funded group health plans are HIPAA-covered entities with independent compliance obligations, separate from any claims administrators/third-party administrators (TPAs) and the plan sponsor. While the plan sponsor's IT systems are used, the self-funded group health plan must undertake its own analysis of the sufficiency of such systems to comply with the plan's obligations under HIPAA.
- The OCR's enforcement action underscores that plan sponsors can face accountability and material financial consequences when the sponsor's self-funded group health plan fails to meet HIPAA requirements, particularly regarding risk analysis and safeguards for ePHI. While plan sponsors may think they don't maintain any ePHI and business associates should have all of the information, it is likely that some level of ePHI is on the plan sponsor's systems due to payment of claims/contracts, information needed for administrative contract pricing or stop loss insurance placement, participant claims/appeals/inquiries to human resources teams or other employees, out-of-network provider demand letters, and communications with business associates related to issues requiring plan sponsor input.

OPERATIONAL STEPS FOR SELF-FUNDED GROUP HEALTH PLANS:

If you operate a self-funded group health plan, the following are key operational steps to consider based on the enforcement actions:

- **Perform a plan-specific risk analysis:** Conduct (or ensure completion of) a comprehensive risk analysis that accounts for systems, applications, and data flows related to the plan's ePHI processing activities, including those performed by third parties such as TPAs. The analysis should explicitly evaluate risks arising from any connections or data sharing with the plan sponsor's corporate systems.
- **Implement and document plan-sponsor firewalls:** Establish clear administrative, technical, and physical safeguards to separate plan information from general employer functions, designed to prevent impermissible uses or disclosures. This is especially important where the same personnel perform both plan administration and sponsor roles.
- **Ensure proper contracting with your business associates:** Confirm current, robust business associate agreements with all TPAs and other applicable vendors that accurately address the scope and nature of ePHI processing by the vendor. Ensure that the business associate agreements include appropriate safeguards for the ePHI processing activities.
- **Maintain thorough documentation:** Maintain documentation of your plan's risk analyses, risk management

decisions, policy versions and distributions, training and training materials, and any incident response analysis for at least six years.

If you sponsor or administer a self-funded group health plan and would like assistance reviewing your current HIPAA compliance program, updating documentation, and/or preparing for potential OCR scrutiny, please contact a member of our Employee Benefits + Executive Compensation Practice Group. Our attorneys regularly counsel plans and plan sponsors on HIPAA compliance, risk analysis requirements, business associate agreements, and responding to OCR investigations. We are happy to help complete these steps and tailor required documentation to your plan's specific structure and operations.

Ashley Golden, a 2026 summer associate with Troutman Pepper Locke who is not admitted to practice law in any jurisdiction, also contributed to this article.

RELATED INDUSTRIES + PRACTICES

- Employee Benefits + Executive Compensation
- Health Care + Life Sciences
- Labor + Employment
- Privacy + Cyber