OCR's HIPAA Settlement With Self-funded Health Plan Highlights Importance of Cybersecurity

On April 23, 2026, the U.S. Department of Health and Human Services' (HHS) Office of Civil Rights (OCR) announced settlements in four ransomware investigations under the HIPAA Security Rule, one of which involved a self-funded group health plan. This development highlights the importance of periodically performing a risk analysis to ensure the appropriate safeguards are in place to protect electronic protected health information (ePHI).

While almost all employer-sponsored health plans are subject to the HIPAA Security Rule, employers that create, receive or maintain ePHI on behalf of their health plans are most vulnerable to cyberattacks. It is especially critical for employers with these health plans to **periodically conduct a risk analysis to ensure the appropriate safeguards are in place to protect ePHI**.

Background

OCR enforces the HIPAA Security Rule, which requires covered entities (health plans, healthcare clearinghouses and most healthcare providers), and business associates to implement administrative, physical and technical safeguards to ensure the confidentiality, integrity, security and availability of ePHI. Performing a risk analysis is a crucial step for regulated entities to comply with the Security Rule. It involves accurately and thoroughly assessing the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by the organization. Going through this process allows a regulated entity to establish appropriate safeguards for its ePHI.

HIPAA Settlement

Star Group, L.P. Health Benefits Plan (SG Health Plan) is a self-funded health plan of a Connecticut-based energy company. In October 2021, SG Health Plan experienced a ransomware attack that compromised the ePHI of 9,316 individuals. Affected ePHI included names, addresses, dates of birth, Social Security numbers and health insurance information, such as member identification numbers, claims data and benefit selection information. SG Health Plan filed a breach report with HHS after the attack, as required by HIPAA.

Following an investigation, OCR determined that SG Health Plan had impermissibly disclosed ePHI and failed to conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity and availability of its ePHI. In the resolution agreement, SG Health Plan agreed to pay $245,000 to OCR and implement a corrective action plan.

Key Compliance Steps

OCR recommends that regulated entities covered by the HIPAA Security Rule take the following steps to prevent or mitigate cyberthreats:

- Identify where ePHI is located in the organization, including how ePHI enters, flows through and leaves the organization's information systems;
- Periodically conduct, and update as needed, a risk analysis and develop and implement a risk management plan to address identified risks and vulnerabilities to the confidentiality, integrity and availability of ePHI;
- Ensure audit controls are in place to record and examine information system activity;
- Implement regular review of information system activity;
- Utilize mechanisms to authenticate information to ensure only authorized users are accessing ePHI;

- Encrypt ePHI in transit and at rest to guard against unauthorized access to ePHI when appropriate;
- Incorporate lessons learned from incidents into the organization's overall security management process; and
- Provide workforce members with regular HIPAA training that is specific to the organization and to the workforce members' respective job duties.
