November 18, 2026

Recent OCR Settlements Highlight HIPAA Compliance Gaps for Employer Health Plans

Two recent enforcement actions by the U.S. Department of Health and Human Services Office for Civil Rights (OCR) highlight why employers that sponsor group health plans should review those plans' HIPAA compliance now. Hiring a third-party administrator (TPA) and maintaining a corporate cybersecurity program can support compliance, but neither automatically addresses all of the plan's obligations. Benefits, IT, and legal teams should confirm who is responsible for each requirement and whether the plan can document that the work has been done.

Recent OCR Enforcement Actions

1. Spencer Gifts LLC Flexible Benefits and Welfare Benefit Plans[1]

On June 18, 2026, OCR announced a $450,000 settlement with Spencer Gifts LLC Flexible Benefits and Welfare Benefit Plans following a ransomware attack affecting the electronic protected health information (ePHI) of 10,023 individuals, including names, addresses, zip codes, phone numbers, email addresses, and Social Security numbers. OCR identified potential failures by the plan to conduct an accurate and thorough risk analysis to protect its network and servers and to implement compliant HIPAA Privacy, Security, and Breach Notification Rule policies and procedures before the breach. The plan agreed to a two-year corrective action plan.

2. Star Group, L.P. Health Benefits Plan[2]

In a settlement signed in January 2026 and announced in April, Star Group, L.P. Health Benefits Plan agreed to pay $245,000 following a ransomware incident affecting 9,316 individuals. OCR identified an impermissible disclosure of PHI and an inadequate risk analysis. The two-year corrective action plan requires an inventory of systems holding ePHI and a review of network segmentation, vulnerability scanning, logging and alerts, patch management, and an analysis of whether adequate separation exists between the plan sponsor and the group health plan.

Practical Steps for Plan Sponsors

Generally, the group health plan is the HIPAA covered entity subject to HIPAA Privacy, Security, and Breach Notification Rule requirements. The employer does not become a HIPAA covered entity merely by sponsoring the group health plan. However, the plan sponsor's personnel may handle PHI on the plan's behalf. While a TPA's compliance program may cover claims processing on the TPA's systems, it may not adequately address the plan's internal practices. Furthermore, corporate IT may protect the employer's network without addressing HIPAA requirements governing plan information. As a result, a plan's reliance on third parties to protect its data may leave gaps in its compliance and expose the plan to liability.

In light of the recent OCR enforcement actions, the following are practical steps group health plan sponsors can take to close compliance gaps.

1. Identify Plan Obligations and Assign Responsibility

Confirm which benefits arrangements are subject to HIPAA and how each is administered. Certain fully insured group health plans that do not create or receive PHI other than summary health information and enrollment or disenrollment information are exempt from most Privacy Rule administrative requirements. However, those limits do not apply to a self-funded arrangement or a plan receiving detailed claims information. For plans subject to the applicable requirements, document the privacy and security official designations and allocate tasks among benefits, IT, legal, and vendors. Identify who approves policies, handles participant requests, and leads incident response.

2. Map Plan Data Flows

Inventory the systems, people, and vendors that create, receive, maintain, or transmit plan ePHI. Include benefits email accounts, shared drives, spreadsheets, laptops, cloud storage, TPA portals, and downloaded reports. Ask benefits personnel to walk through real workflows, including claims assistance and appeals. Distinguish HIPAA plan information from employment records held by the plan sponsor in its employer capacity. Use the inventory to identify unnecessary copies and access to plan data.

3. Confirm Risk Analysis Covers Plan Data

Review the scope and results of the most recent risk analysis. Although a corporate cybersecurity assessment, penetration test, or TPA assurance report may provide useful evidence, in order to comply with HIPAA, the plan needs a documented analysis addressing risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI. An integrated corporate assessment can serve that purpose if it adequately covers the plan's information, systems, and workflows. Any necessary remediation tasks should be documented with appropriate deadlines. This risk analysis should be revisited as systems, vendors, or operations change.

4. Review Vendor Obligations

Review service agreements and business associate agreements. Confirm who handles participant access requests, privacy notices, incident investigation, and breach notifications, and what obligations remain with the plan. Seek prompt incident reporting, cooperation, and access to the information needed to assess an event and meet deadlines. Review available security documentation and follow up on any material concerns.

5. Review Plan Policies and Procedures

Where appropriate, review whether there is adequate separation between the plan sponsor and the group health plan by verifying that plan documents contain HIPAA privacy and security provisions and that the sponsor has provided the necessary certification before receiving PHI for plan administration. Identify the appropriate personnel and restrict access to only their plan administration functions, including reviewing shared-folder permissions and network segmentation. Confirm that PHI received for plan administration is not used or disclosed for employment decisions or to administer other employee benefit plans.

In addition, review and update written privacy, security, and breach response procedures to reflect actual operations and ensure that benefits personnel receive appropriate HIPAA training.

---

[1] See Resolution Agreement, available at https://www.hhs.gov/sites/default/files/ocr-ra-cap-spencer.pdf.

[2] See “SG Health Plan Resolution Agreement and Corrective Action Plan,” U.S. Dep't of Health and Human Servs., available at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ra-cap-with-sg-health-plan/index.html.

Authors



Brendan J. Butler
Counsel

Hartford, CT | (860) 275-0277

bbutler@daypitney.com



Stephanie M. Gomes-Ganhão
Associate

Hartford, CT | (860) 275-0193

sgomesganhao@daypitney.com



Thomas F. J. O'Mullane
Partner

Parsippany, NJ | (973) 966-8413

tomullane@daypitney.com



William J. Roberts
Partner

Hartford, CT | (860) 275-0184

wroberts@daypitney.com