

McGohan Brabender's Compliance IN MOTION

June 2026

HIPAA Enforcement Against a Self-Funded Employer Plan

On April 23, 2026, the HHS Office for Civil Rights (OCR) announced a \$245,000 settlement with the Star Group, L.P. Health Benefits Plan ("SG Health Plan"), a self-funded employer-sponsored group health plan, after a 2021 ransomware attack exposed the protected health information (PHI) of over 9,300 participants. The employer did not have a Risk Analysis to identify ways Protected Health Information (PHI) could be compromised, did not have a Risk Management Plan with robust policies and procedures to vigorously protect PHI from attack, and likely had access to more PHI than the minimum necessary they truly needed for plan oversight and operations.

The announcement followed OCR's most recent Annual Report to Congress on Breaches of Unsecured Protected Health Information (2023 Breach Report), which shows hacking drove 81% of large breaches in 2023 and affected roughly 113 million people.

Health care providers and Business Associates continue to dominate the violations reflected in each year's report to Congress, which seems to give plan sponsors a false sense that comprehensive HIPAA compliance can wait. One lost or stolen device or one hacking incident is all it takes to risk violating HIPAA, and OCR can and will hold the plan sponsor directly accountable.

WHO THIS APPLIES TO:

- Employer sponsors of self-funded or level-funded group health plans, including medical, dental, vision, and prescription drug plans, Health Flexible Spending Arrangements (FSAs), and Health Reimbursement Arrangements (HRAs), that handle, create, receive, maintain, or transmit PHI beyond enrollment, disenrollment, and summary health information for purposes of plan administration.
- Business Associates of those plans, including third-party administrators (TPAs), claims processors, pharmacy benefit managers (PBMs), brokers and consultants handling PHI, IT vendors, and cloud service providers.

Excluded from the definition of “health plan” entirely under 45 CFR § 160.103 are group health plans with fewer than 50 participants that are self-administered by the employer that established and maintains the plan. Note, it is quite rare for an employer to self-administer a self-funded plan such as an HRA without the help of a TPA, so this exception does not apply in most cases.



GO DEEPER:

The 2023 Breach Report shows hacking and IT incidents drove 81% of large breaches, which affected 96% of the 113 million impacted individuals. Network servers were the most common location of compromised, unsecured PHI.

Health plans filed 116 of the 732 large-breach reports (16%), accounting for roughly 14.6 million affected individuals.

OCR resolved seven breach investigations in 2023 with resolution agreements and corrective action plans, collecting just over \$6 million in settlements. Across investigations, OCR repeatedly identified the same HIPAA Security Rule failures:

- Incomplete or missing risk analyses,
- No functioning risk management plan,
- No information system activity review,
- Weak or absent audit controls, and
- Weak authentication procedures (especially the lack of multi-factor authentication for remote access).

When Star Group, L.P. was hacked, OCR’s investigation found they were deficient in these same areas.

The SG Health Plan Settlement

Star Group, L.P. is a Connecticut-based energy provider. Its self-funded employee benefits plan filed a breach report with OCR in October 2021 after an unauthorized actor deployed ransomware on the plan’s information system and exfiltrated PHI for over 9,300 individuals. The exposed PHI included names, addresses, dates of birth, Social Security numbers, member identification numbers, claims data, and benefit selection information.

OCR’s investigation found two violations:

- Impermissible disclosure of PHI in violation of 45 CFR § 164.502(a); and
- Failure to conduct an accurate and thorough Risk Analysis under 45 CFR § 164.308(a)(1)(ii)(A)

The plan had to pay \$245,000 within seven days and enter into a 2-year Corrective Action Plan (CAP) that requires the plan to:



- Build a complete inventory of all facilities, equipment, data systems, and applications that contain, store, transmit, or receive electronic PHI (ePHI);
- Conduct an enterprise-wide Risk Analysis that addresses network segmentation, network infrastructure, vulnerability scanning, logging and alerts, and patch management;
- Review whether adequate separation exists between the plan sponsor (the employer) and the group health plan, as required under 45 CFR § 164.504(f);
- Develop a risk management plan to address every risk identified;
- Revise written HIPAA Privacy, Security, and Breach Notification policies and procedures, submit them to OCR for approval, and distribute them to the workforce;
- Train workforce members on the approved policies within 60 days of approval and at least every 12 months thereafter;
- File a training implementation report and annual compliance reports with OCR; and
- Investigate and report any workforce non-compliance ("Reportable Events") to OCR.

Why This Settlement Matters for Self-Funded Employers

Most OCR settlements involve providers, hospital systems, or Business Associates such as TPAs. Direct enforcement against a self-funded employer plan is rare, which is what makes this case worth attention.

The HIPAA Security Rule applies directly to the plan, and in a self-funded arrangement the employer facilitates the plan's legal obligations. Hiring a TPA or PBM as a Business Associate to administer claims does not move Security Rule responsibility off the plan. The HIPAA Privacy Official in this case was Star Group's Director of Employee Benefits, which is typical for self-funded plans and is the practical reason the benefits team and the company's IT/information security team have to work together on safeguards for ePHI.

The CAP also requires SG Health Plan to review whether adequate separation exists between the plan sponsor and the group health plan. That is the 45 CFR § 164.504(f) "firewall" requirement, which limits the plan sponsor's use of PHI to the minimum necessary needed for plan administration functions, and obligates the plan documents to identify the specific employees who may receive PHI and for what purposes. Many self-funded plans treat the firewall language as a one-time plan document insertion. OCR's CAP confirms it is an ongoing compliance obligation.

This is actually a core issue worth noting:

- **Employers almost never have a true need for PHI. Deidentified claim detail is typically the minimum necessary to oversee the plan and strategize on its future. Had this employer only kept deidentified health information, a breach report would not have been required when hacked since they would not have any PHI.**



- For any PHI that was truly needed, a reportable breach would not have been necessary if that PHI had been properly secured (encrypted). Breach notification requirements are triggered when the PHI is unsecured (not encrypted).

Three Other Settlements Announced the Same Day

OCR announced SG Health Plan's settlement alongside three other ransomware resolutions on April 23, 2026, totaling \$1,165,000 in collected penalties:

- Regional Women's Health Group, LLC (d/b/a Axia Women's Health): \$320,000 (almost 38,000 individuals affected)
- Assured Imaging Affiliated Covered Entities: \$375,000 (almost 245,000 individuals affected)
- Consociate, Inc. (d/b/a Consociate Health), a TPA serving group health plans: \$225,000 (over 136,000 individuals affected)

Consociate is a TPA for employer-sponsored benefit plans. Plans that use TPAs should not assume the TPA's settlement closes the matter for the employer. The plan keeps its own Security Rule obligations as a Business Associate, regardless of how the breach started or which entity OCR happened to settle with first. Plan sponsors should regularly review their Business Associates' compliance with HIPAA and document what they find.

HIPAA Security Rule Updates Expected This Month

OCR published a Notice of Proposed Rulemaking (NPRM) on December 27, 2024 to update the HIPAA Security Rule for the first time since 2013. OCR's Spring 2025 Unified Agenda lists May 2026 as the target for a final rule, so we are expecting it soon but know federal regulators routinely miss those self-imposed deadlines.

Key proposals to watch:

- Elimination of the "addressable" versus "required" implementation specification distinction. Specifications currently labeled "addressable" (those that allow plans to document a reasonable alternative) would become required for every regulated entity.
- Mandatory multi-factor authentication, encryption of ePHI at rest and in transit, network segmentation, and vulnerability scanning at set intervals.
- Stricter audit log review, regular technical testing, and expanded incident response requirements.
- A required written technology asset inventory and network map documenting where ePHI lives and how it moves through the plan's systems.
- Annual compliance audits.

What Plan Sponsors Should Do

Employers with access to PHI, which is typically those with a self-funded health plan or a claims analytics data feed for their fully insured plan, should document regular, robust diligence to comply with HIPAA Privacy and Security. Breaches are increasing in frequency and severity and are largely preventable.



- Identify through a written **HIPAA Risk Analysis** where PHI is accessible and vulnerable. Every system, partner, and employee should be named with an explanation of PHI access for each.
- Build a **risk management plan** tied to the Risk Analysis. Identifying risks without addressing them is a separate violation. Detailed **policies and procedures** must outline exactly how PHI will be regularly and carefully protected, employees responsible for operating the plan **must be trained** on those policies and procedures, and the employer must hold employees, partners, and systems accountable.
- Confirm the plan documents include the 45 CFR § 164.504(f) **plan sponsor firewall language** and that the employees listed match current job functions. The vast majority of employers do not actually need PHI to properly oversee their plan and strategize for the plan's future. Always ensure the **minimum necessary** is given to the employer, which should be completely deidentified health information in most cases.
- Verify **Business Associate Agreements** (BAAs) are in place with every vendor that creates, receives, maintains, or transmits PHI on behalf of the plan, confirm the BAAs reflect current Security Rule expectations, and **document regular auditing** that demonstrates Business Associates are diligent in their HIPAA compliance.
- Coordinate with the **information cybersecurity team**. The benefits department alone cannot satisfy the Security Rule. Multi-factor authentication, encryption, audit logging, patching, backup, proactive cybersecurity protections, and incident response all sit with IT.
- Track the final HIPAA Security Rule. Once published, expect a tight implementation window. Each piece may be costly, including MFA deployment, encryption of ePHI at rest, network segmentation, the written asset inventory, routine testing of off-site backups at that physical location, and more.

Consequences of Non-Compliance:

- HIPAA civil money penalties follow a four-tier structure based on culpability (lack of knowledge, reasonable cause, willful neglect-corrected, willful neglect-not corrected), with per-violation amounts indexed annually.
- Resolution agreements with corrective action plans. SG Health Plan's settlement is \$245,000 payable within 7 days, plus two years of OCR monitoring, document submissions, mandatory policy approvals, and annual reporting. SG likely also had to pay a ransom and pay for credit monitoring for over 9,300 individuals since SSNs were compromised.
- State attorneys general have parallel HIPAA enforcement authority under HITECH § 13410(e); a single breach can produce both federal and state enforcement actions.
- Mandatory individual breach notification under 45 CFR § 164.404, Secretary notification under 45 CFR § 164.408, and media notification for breaches affecting more than 500 residents of a state under 45 CFR § 164.406. Notification costs (mailings, credit monitoring, call centers, legal counsel) routinely exceed the OCR resolution amount.



PCORI Fees Due by July 31, 2026

Each year by July 31, employers sponsoring certain self-funded health plans must file and pay an annual fee to the IRS to fund the Patient Centered Outcomes Research Institute (PCORI). Employers must report the fee on the **second quarter** IRS Form 720.

The IRS usually releases the second quarter Form 720 after Memorial Day. Employers can gather their enrollment counts from their third-party administrator (TPA) for their self-funded health plan year that **ends** during calendar year 2025, and can take care of the filing and payment using the updated Form 720 anytime between when the new form is published and July 31.

WHO THIS APPLIES TO:

- Employers sponsoring any self-funded medical plan, including a level-funded plan, a Health Reimbursement Arrangement (HRA) under certain circumstances, or an Individual Coverage HRA (ICHRA).
- Insurance carriers are responsible for PCORI fees for fully insured plans.

Exempt: Excepted benefits such as stand-alone vision or dental, HSAs or health FSAs that qualify as excepted benefits.



GO DEEPER:

The PCORI fee must be reported each year on the second quarter version of IRS Form 720 and paid electronically or mailed to the IRS using the Form 720-V payment voucher.

Employers that are subject to PCORI fees but no other types of excise taxes should file Form 720 only for the second quarter. In other words, no filings are needed for the other quarters, only the second quarter.

For plan years ending in 2025 before October 1, the PCORI fee due this July is \$3.47 per covered life. For plan years ending between October 1, 2025 and December 31, 2025, the PCORI fee due this July is \$3.84 per covered life.

How to Calculate the Number of Covered Lives

The PCORI fee is based on the number of employees, spouses and dependents that are covered by the plan (for an HRA, it is based only on the number of enrolled employees, not spouses and dependents). The employer can use the actual count method, snapshot method, snapshot factor method, or Form 5500 method to determine the average number of covered lives. Below is more information on each of the approved counting methods:

Actual Count Method: This method calculates the average of covered lives by adding the number of lives covered each day of the plan year divided by the number of days in the plan year.



For example, a plan that starts on January 1 calculates the sum of covered lives (*including spouses and dependents*) as 676,772 divided by 365, which is 1,854.17. Thus, the PCORI fee for plan year ending in 2025 is 1,854.17 times \$3.84, or \$7,120.01.

Snapshot Method: This method calculates the average by adding the total number of lives covered on a date during the first, second, or third month in each quarter, or an equal number of dates during each quarter, and dividing by the number of dates. The date chosen in each quarter must be within ± 3 days of the date used in other quarters.

Example for a calendar year plan:

Date	Count	Total Fee	
1/4/25	2,000		
4/5/25	2,100		
7/5/25	2,050		
10/4/25	2,050		
Total	$8,200 \div 4 = 2,050.00$		$\times \$3.84 = \$7,872.00$

Snapshot Factor Method: This method uses the number of participants with other than self-only coverage (e.g., family, EE + spouse, EE + child, etc.) on the designated quarterly dates discussed above under the snapshot method, multiplied by 2.35, and adds the number of employees on each date with self-only coverage to come up with the enrollment total for each date.

Example for a calendar year plan:

Date	Count Non-Single	+ Count Single	Total Fee
1/4/25	$800 \times 2.35 = 1,880.00$	$+ 600 = 2,480.00$	
4/5/25	$800 \times 2.35 = 1,880.00$	$+ 608 = 2,488.00$	
7/5/25	$808 \times 2.35 = 1,898.80$	$+ 610 = 2,508.80$	
10/4/25	$808 \times 2.35 = 1,898.80$	$+ 610 = 2,508.80$	
Total		$9,985.60 \div 4 = 2,496.40$	$\times \$3.84 = \$9,586.18$

Form 5500 Method: This is based on the average number of covered lives reported on Form 5500 for the plan year. Employers can only use this method if the Form 5500 is filed no later than the due date for the PCORI fee imposed for that plan year. In other words, if the plan year ending in 2025 will not have the 5500 filed by July 31, 2026, this method cannot be used.

Under this method, the total number of lives is calculated by adding the total participant counts at the beginning and end of the year and dividing by 2 for a plan that only offers single coverage. If a plan offers single coverage along with other coverage (e.g., family coverage), the total number of lives is determined by adding the total participant counts at the beginning and end of the year (without dividing by 2).



Example for a calendar year plan:

Date	Count		Total Fee
1/1/25	1,400		
12/31/25	1,418		
Total	2,818.00		× \$3.84 = \$10,821.12
		2,818 ÷ 2 = 1,409.00	(or \$5,410.56 single-only)

What if the employer did not pay or made a mistake in prior years?

The IRS has not provided express guidance on how to address late PCORI payments. Based on the forms and instructions, it appears that employers should use prior year forms (found [here](#)) that correspond to the due date of the fee. If the IRS notifies the employer plan sponsor of their intent to impose a penalty, the group should have the opportunity to appeal if the failure was due to reasonable cause.

A mistake to a previous submission can be corrected using [Form 720-X](#).

Where to get assistance with calculating the number of covered lives?

Employers should rely on the TPA to assist with the calculation. Even if the employer uses a TPA or a vendor to assist with the calculation, the PCORI fee for a self-insured plan, ICHRA or HRA is the responsibility of the plan sponsor and must be paid by the employer to the IRS directly. Failure to file likely carries the same penalty for failure to pay other taxes due on Form 720.

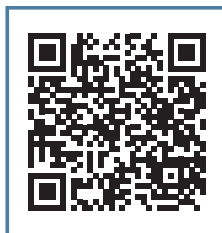
MHPAEA Lawsuit Allowed to Proceed

Another lawsuit alleging violation of the Mental Health Parity and Addiction Equity Act (MHPAEA) is underway, and the motion to dismiss was [denied](#). BCBS of Illinois attempted to claim their requirement for 24/7 on-site nursing in residential treatment centers (RTC) mirrors the 24/7 on-site care requirement in skilled nursing facilities (SNFs), but the court pointed out the carrier only requires SNFs to be licensed by the appropriate government entity and operate within the scope of that license which means it is not necessarily a requirement that they have 24/7 on-site nursing. This means they impose a more stringent requirement on RTC than they do on SNF, which could potentially violate MHPAEA and the case is allowed to proceed. The lawsuit is filed against both the TPA and employer.

Waiting for HSA Indexing for 2027

Surprisingly, HSA indexing has not been announced for 2027. We will publish an alert when the indexed amounts are published.





[CLICK HERE](#) OR SCAN
QR CODE TO VIEW PAST
COMPLIANCE IN MOTION
NEWSLETTERS

