Insights, News & Events

8 KEY HIPAA COMPLIANCE ITEMS FOR BUSINESSES WITH SELF-INSURED HEALTH PLANS

Insights
Mar 2, 2026

8 Key HIPAA Compliance Items for Businesses with Self-Insured Health Plans

Are you a business with a self-insured group health plan? Did you know that it could make part of your business subject to HIPAA? Employers that sponsor self-insured group health plans are subject to complex compliance rules that span federal privacy and security requirements, state law obligations, and evolving regulatory expectations. This Insight highlights how non-health-related businesses can become subject to HIPAA and covers eight key compliance items – including upcoming regulations that will impose additional obligations.

How HIPAA Applies

For most private-sector employers, a self-insured group health plan is also governed by the Employee Retirement Income Security Act of 1974 (ERISA), making it subject to ERISA's fiduciary and plan administration requirements. At the same time, HIPAA's privacy and security rules apply directly to group health plans as covered entities, regardless of whether ERISA applies.

Employers become subject to HIPAA obligations when they sponsor a self-insured group health plan because the plan itself is a "covered entity" under HIPAA. Even if an organization utilizes a third-party administrator (TPA), the employer still maintains the compliance risk when they receive, maintain, or transmit PHI for the benefit of the plan.

Related People

Jennifer S. Kiesewetter
Partner

615.488.2905

Jillian Seifrit, CIPP/US
Associate

610.230.6129

The HIPAA regulations will only apply to the health plan and not to the employer's general business operations. Organizations should keep all health plan activities and data separate from their broader general operations.

When a health plan is subject to ERISA, the plan documents must address both ERISA governance requirements and HIPAA privacy obligations. If the employer will access PHI for plan administration purposes, the plan documents must be updated to reflect this, including provisions that limit how the employer may use and disclose that information and establish the necessary safeguards and certifications under federal law. A plan that meets ERISA's governance standards but omits these HIPAA provisions is still out of compliance.

What is PHI In the Context of Self-Insured Health Plans?

Whether employee data is PHI is a key distinction. Employees provide their sensitive information to employers for many reasons. For example, as part of the hiring process, employees may provide employers with their name, address, Social Security number, driver's license number, and financial account information. Further, employees may be required to take a drug test or submit medical certifications from doctors to support request for leave under FMLA. All this sensitive information is not considered PHI if an employer is using this medical information in their role as an employer, and not for the purposes of administering its self-insured health plan.

On the other hand, any identifiable information that is utilized as part of the plan administration is PHI, and this is not limited to medical information.

8 Core HIPAA Compliance Items for Self-Insured Health Plans

1. Determine if your organization receives, maintains, or transmits PHI. This involves documenting where PHI enters, flows, and is used within your organization. If your organization has a self-insured plan, you are likely receiving at least some PHI from employees. Employers should also confirm whether any exemptions apply, such as for small, self-administered plans with fewer than 50 participants or for excepted benefits such as certain standalone dental or vision plans. While most self-insured medical plans will not qualify for these exemptions, the analysis should be documented.

Daniel Pepper, CIPP/US

Partner

303.218.3661

Service Focus

Counseling and Advice

Data Protection and Cybersecurity

Employee Benefits and Tax

Privacy and Cyber

Industry Focus

Healthcare

2. Don't rely solely on TPA's policies. Many organizations assume that they can rely on their TPA's policies; however, if your organization receives PHI from the plan, the organization itself needs to have its own HIPAA Privacy and Security policies.

3. Designate a HIPAA Compliance Officer. The responsibilities of this individual depend on the organization's size and whether they are also designated as the Privacy and/or the Security Officer.

4. Fulfill Privacy Rule obligations, including:

- **Implement policies on uses and disclosures of PHI.** The privacy rule focuses on limiting the circumstances where an individual's PHI may be used or disclosed.
- **Maintain a Notice of Privacy Practices (NPP) for your plan participants.** Recent NPP requirements are effective February 16, 2026, so you must act quickly to comply. Learn more here.
- **Note:** Failure to comply with the HIPAA Privacy Rule can come with steep fines. The penalty amount **per violation** can range from **$127 - $63,973**.

5. Comply with the Security Rule and stay tuned for updates. Federal officials proposed updates in December 2024 to HIPAA's Security Rule (which would be the first significant HIPAA update since 2013) that aim to address the evolving cybersecurity landscape. We previously covered the details and offered employers a suggested gameplan, but here are some key points from the proposed rule:

- Strengthen protections for ePHI by aligning HIPAA with security best practices such as NIST.
- Expand covered entities' and business associates' obligations to protect against internal and external threats.
- Change "addressable" standards to "required" status.
- Emphasize documentation, testing, and ongoing review.
- For a detailed overview of the updates to the Security Rule and our suggested gameplan, please see our previous Insight.

6. Implement a business associate agreement (BAA) when required. Every vendor that your organization works with regarding the plan and that handles PHI must execute a BAA. This includes your TPA and cloud vendors. You should also ensure that these vendors are securely handling data.

7. Follow breach notification rules. The plan must follow HIPAA's breach notification requirements and have written procedures to respond to a breach. HIPAA requires notice to individuals within 60 days of discovering a breach. Additionally, the plan must notify the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR) within 60 days of discovery if 500 or more individuals are impacted or if fewer than 500 individuals are impacted, not later than 60 days after the end of the calendar year. Employers should also evaluate whether state data breach notification laws apply. Self-insured status does not remove those obligations, and ERISA preemption will not prevent compliance with state data breach requirements.

8. Ensure ERISA fiduciary and cybersecurity oversight. HIPAA's privacy and security rules set the baseline for protecting PHI. If the health plan is governed by ERISA, fiduciaries have an additional responsibility. The US Department of Labor has made clear that ERISA's duties of prudence and loyalty extend to cybersecurity risk, including vendor selection, monitoring, and incident response. These fiduciary expectations are separate from, and in addition to, HIPAA's regulatory requirements. Even where an employer has implemented HIPAA Security Rule safeguards, ERISA fiduciary oversight may require additional attention to governance and vendor monitoring.

Conclusion

Fisher Phillips will continue to monitor developments and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on our Data Protection and Cybersecurity Team or our Employee Benefits and Tax Team.