

Does Hiring a Business Associate to Conduct Electronic Health Plan Transactions Absolve a Health Plan of HIPAA Liability?

EBIA Weekly (December 11, 2025)

QUESTION: We sponsor a self-insured health plan for our employees. A TPA handles day-to-day administration of the plan, including processing claims and making payments to health care providers. We understand that HIPAA establishes standards for electronic health care transactions. If the TPA fails to comply with those standards, is the plan potentially liable under HIPAA?

ANSWER: If your company sponsors a self-insured health plan and hires a TPA to handle administrative tasks—such as processing claims and making payments—your health plan is still responsible for complying with HIPAA's electronic transaction standards. The electronic transaction standards apply to a range of financial and administrative activities, and they must be conducted in accordance with detailed technical standards and operating rules. Even if a health plan delegates duties to third parties, the health plan remains ultimately responsible for compliance. Typical health care transactions a TPA may perform on a health plan's behalf include making or responding to requests for information about eligibility and coverage (e.g., from a provider to a health plan, or from one health plan to another); responding to claim status inquiries from providers; processing providers' requests for payment from the plan; and making payments from the plan to providers, including electronic funds transfers.

When performing HIPAA-covered health care transactions on behalf of a health plan, the TPA is considered a HIPAA business associate. Health plans, as HIPAA covered entities, must contractually require their business associates to comply with the electronic transaction standards and operating rules. However, business associates do not have direct liability for noncompliance, and engaging a business associate does not relieve a covered entity from its own obligation to comply. Thus, if your TPA fails to comply with the electronic standards and operating rules, HHS may seek recourse against your health plan for the TPA's noncompliance.

Moreover, a business associate's noncompliance with an electronic transaction standard could be used as evidence of a covered entity's failure to require the business associate to comply, even if a contract between the covered entity and a business associate obligates the business associate to comply with all applicable requirements. Accordingly, performing due diligence when hiring business associates and monitoring their performance are important elements of demonstrating that a plan fiduciary has acted prudently and may avoid having to cure HIPAA breaches or terminate contracts.

Note that different liability rules for business associates apply under HIPAA's privacy and security standards. Consistent with the HITECH Act, business associates are directly liable for compliance with the security standards and some of the privacy standards but not the electronic transaction standards, which remain the responsibility of the health plan. For more information, see EBIA's HIPAA Portability, Privacy & Security manual at Sections XXIV ("Business Associate Contracts") and XXXII ("Electronic Transactions and Code Sets").

Contributing Editors: EBIA Staff.
