MYTH: A business associate's scope of liability is determined by the terms of its business associate agreement with a covered entity.

FACT: Under the HITECH Act's amendments to HIPAA, business associates are directly liable for compliance with the Privacy and Security Rules.

The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)[1] changed how HIPAA applies to business associates. These changes were codified in the omnibus Final Rule published by HHS on January 17, 2013.[2]

Prior to HITECH, the HIPAA Privacy, Security, and Enforcement Rules did not directly govern or penalize business associates for noncompliance; rather the business associate contracts between a covered entity and a business associate governed enforcement and penalties.

Now, specific requirements of the Privacy Rule apply to business associates and make them directly liable for noncompliance with those requirements in addition to any requirements included in their business associate agreements with covered entities.

Moreover, the administrative, physical, and technical safeguard requirements in the Security Rule now directly apply to business associates in the same manner as they apply to covered entities, along with HIPAA's policies, procedures, and documentation requirements.

Finally, HIPAA's enforcement process (including civil and criminal penalties for violations of the Privacy and Security Rules) now directly applies to business associates in the same manner as it applies to covered entities.

Business associates are not required to meet all requirements of the Privacy Rule. While the substantive provisions that relate to the use and disclosure of protected health information (such as the requirements for disclosure to an individual and for compliance with the minimum necessary standard) now apply to business associates, they are not required to provide a notice of privacy practices or designate a privacy official unless a covered entity has obligated the business associate to do so on its behalf. A business associate may use or disclose protected health information for proper management and administration purposes and to provide data aggregation services to the covered entity if such uses and disclosures are permitted in the business associate agreement.

For More Information:

- See a sample business associate agreement.
- Learn about state and federal laws related to privacy.
- Read our overview of HIPAA and related resources.

Follow us on Twitter at @HealthInfoLaw

---

[1] American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009), Division A, Title XIII and Division B, Title IV, Health Information Technology for Economic and Clinical Health Act (HITECH Act) (codified at 42 U.S.C. § 17930, et seq).

[2] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg. 5566 (January 25, 2013) (to be codified at 45 CFR pts 160 and 164).