Protected health information

How to respond when asked to sign a business associate agreement

INTERVIEWED BY ROGER VOZAR

REBECCA PRICE
Associate
Kegler, Brown, Hill and Ritter, Co., L.P.A.

(614) 462-5411
rprice@keglerbrown.com

WEBSITE: To learn more about Kegler's health care regulation practice, visit www.keglerbrown.com/practice-areas/health-care-regulation--hit.

Insights Legal Affairs is brought to you by **Kegler, Brown, Hill & Ritter**

The U.S. Department of Health and Human Services (HHS) released a final Omnibus Rule this year creating higher standards concerning protected health information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA).

As a result, hospitals and other health care providers are asking businesses working with them to sign business associate agreements, even in situations where they may not be applicable, says Rebecca Price, an associate at Kegler, Brown, Hill & Ritter, Co., L.P.A.

"It becomes problematic for businesses if you are not a business associate as defined under HIPAA, and you are asked to sign a business associate agreement," Price says. "There are some very specific compliance requirements you don't want to endure the cost and hassle of unless it's really necessary."

Smart Business spoke with Price about business associate agreements and what to do if you're asked to sign one.

What changed with the final Omnibus Rule?

One of the biggest differences is lower-tiered subcontractors have direct liability for HIPAA compliance. Also, the terms and definitions provide more clarity regarding what is expressly required of a business associate; prior rules had gray areas.

HIPAA was unveiled in 2003, and there was a major change in 2009 that dealt with business associates and electronic information. The final Omnibus Rule is a significant document expected to have sizable financial impact on the economy.

How do you determine if you're a business associate?

It's a matter of determining what work you're doing with the covered entity — the health care provider, health care clearinghouse or insurance company. Generally, any time you might have access to PHI, you are a business associate, which can include companies that provide legal, accounting, consulting, administrative or financial services for a covered entity. Anyone who sees any type of PHI is subject to HIPAA, with very few exceptions.

Covered entities want to spread the risk, and as a matter of course some are including business associate agreements as part of their standard paperwork. But there are companies doing business with covered entities, like a custodial company, that do not need business associate agreements.

What is required of a business associate?

You need a HIPAA compliance program, including designating a security official and policies and procedures. You have to audit certain data, such as the use and disclosure of PHI. There's a long list of administrative requirements. It's a very involved process.

Companies wanting to do business with a covered entity need to give some thought about whether to sign a business associate agreement. It's tempting to say you have to sign one to get the business, even if you're not really a business associate. But be intentional about your decision. If you're going to have access to PHI, figure in the cost of being HIPAA compliant because it's going to come off of the profit.

The final Omnibus Rule extends HIPAA compliance requirements to subcontractors doing business with business associates, such as a copy service or a company providing document management services to a law firm. In certain situations, if PHI is copied, the law firm needs to have a business associate agreement with the copy service, because the copy service has had access to the PHI and even those copy machines now store data. It's very complicated, and the requirements keep going downstream.

Can you hire someone to provide a compliance program?

Certainly there are attorneys that supply HIPAA compliance programs. There also are non-attorney programs, but be careful not to go with something that is just forms because the amount of scrutiny anticipated under the Omnibus Rule suggests you need to pay attention to details and create a program that fits your business.

The HHS Office of Civil Rights has said it will be auditing business associates, so there is a greater risk of operating any business dealing with PHI without a comprehensive HIPAA program. Penalties range between $100 and $50,000 for the first violation. If there is a second violation in the same calendar year, fines jump to $1.5 million. So, there is a lot at stake for health care providers and their business associates. ●