DataMotion™

HIPAA/HITECH Update: Covered Entity vs. Business Associate

In 2009, Subtitle D of the HITECH Act updated HIPAA in ways that affect thousands of businesses, many of which don't even realize they're now subject to HIPAA regulations. As of September 2013, anyone with any level of exposure to protected health information (PHI), even if they've never been near a hospital or a patient, is subject to the same privacy standards as the doctors and medical establishments themselves.

The original HIPAA provisions applied to covered entities, which are the individuals or entities that actually interact with the patient. This includes doctors, nurses, lab techs, and hospitals. The HITECH Act established a whole new class of businesses that are subject to HIPAA provisions: **business associates**, which comprise any contractors who might have access to that patient data.

For example, the cleaning crew that comes in at midnight never see a patient, but because there might be patient charts in the doctor's inbox, they potentially have exposure to patient data and must adhere to HIPAA privacy standards. The law would also apply to a doctor's tax accountant, who might live in another state and may never have set foot in the office. Because they see where the doctor's money comes from, they could be exposed to patient information.

And it's not just the contractors who are affected: the definition of a business associate, as created by the HITECH Act, extends to infinite levels of subcontractors. This means that the cleaning crew's office manager—and their virtual assistant in Singapore—are subject to the same regulations. While it may be unlikely that someone that far down the chain would receive any confidential patient information, they now share in the liability should anything be exposed—which means that they share in the responsibility for ensuring best practices and techniques to protect sensitive information.

Becoming a Business Associate

So what does this mean for you? First, if you qualify as a business associate under the HITECH Act, you should have a contract with the covered entity (or the business associate who hired you) that codifies your status as such, identifies your level of exposure, defines the appropriate uses of the data to which you may be exposed, and establishes the safeguards you are using to prevent unauthorized exposure. This contract should also include standards for breach notification, in case an unauthorized exposure occurs. (More information on this, including a sample contract, is available here.)

If you don't have this type of contract, but are dealing with medical establishments (or with a business that deals with medical establishments), you should get one immediately. The final omnibus ruling for the HITECH Act went into effect in September 2013, so you may already be in violation. Worse, if you have any kind of contact with PHI and still have gaps in your security measures, you are exposing yourself (and all the people whose data you interact with) to potential attacks, and may be subject to criminal investigation and penalties.

There is another issue at play here—the confidence of your business partners or clients. Patients want to know that their data is safe, and they won't go to a doctor who has compromised their information. This means that doctors won't hire vendors who have compromised information either, and most won't even take the chance on a company that doesn't have a strong privacy program in place.

Any company that qualifies as a business associate under HIPAA can take steps toward compliance by adopting an email encryption solution. Encrypting email has a host of benefits, for regulatory compliance and beyond:

- It reduces the risk of a data breach and the customer loss and bad PR that might ensue.
- It allows you to take advantage of the fastest, most efficient communication medium (email) in a safe and compliant manner, thereby reducing your dependence on legacy systems like fax and regular mail.
- It can help prevent fines related to non-compliance.
- It reduces your legal liability in the event of a data breach.

Given the long tail of liability created by the HITECH Act, healthcare professionals must be diligent about privacy and security—especially with regard to their business associates. If you want to continue working with healthcare professionals, even indirectly, make sure you have the proper contracts in place and use an email encryption program to protect yourself, your healthcare clients, and their patients from malicious attacks.

DataMotion

200 Park Avenue, Suite 302
Florham Park, NJ 07932
800-672-7233
www.datamotion.com
@DataMotion