Healthcare IT News

How to Succeed as a HIPAA Business Associate

BAs' average cost from a data breach is $1 million

Today, everyone involved in the healthcare industry, even remotely, needs to know their responsibilities regarding data privacy and security, because everyone is potentially held accountable by customers, regulators, the courts, and their business partners. Under the HIPAA Final Rule, business associates of healthcare organizations – known as "covered entities" or "CEs" – are being held responsible for following privacy regulations, and facing fines if they don't.

BAs are now being audited by the Department of Health and Human Services' Office for Civil Rights, and the 5th Annual Benchmark Study on Privacy & Security of Healthcare Data from Ponemon Institute found that business associates' average cost from a data breach is $1 million. So no matter the size of your business or how far removed you are from the front lines of medical care, you must know your responsibilities and how to handle protected healthcare information.

As a BA, you have direct obligations to federal regulators to follow the Privacy, Security and Breach Notification Rules of the HITECH Act and the HIPAA Final Rule. Your BA Agreement clarifies areas where you have to work with your client (the covered entity) under certain circumstances, most specifically, breach notification. If you discover an incident that you think is a data breach, you're obligated to notify your client. Your BAA likely outlines the requirements, such as the timeframe for this notification, the content of breach and patient notifications, and who would bear the costs if your organization caused the breach.

As of Sept. 22, 2014, all CEs were required to have these contracts in place with all of their BAs, and that is one of the things that OCR will be checking as it does audits of randomly chosen healthcare organizations over the next few years. In fact, the law now requires that subcontractors with whom BAs share PHI must also have agreements, so there could be a web of agreements between CEs and BAs, between BAs and their subcontractors, and sometimes between the contractors themselves.

A special security contract may sound intimidating to a BA that is a mid-sized or smaller business, but having a BA Agreement in place is actually a win-win.

First, it spells out what the business associate needs to do in order to comply with the

HIPAA requirements, and the contracting process may trigger discussions or reviews that lead to improved data security and help prevent future data breaches.

Second, knowing exactly what is expected helps a BA maintain a good business relationship with valued customers. If a CE knows of a breach or violation by a BA, the CE is required to take reasonable steps to remediate the breach or end the violation. If that doesn't happen, they must end the contract. In case a breach does happen, if the BA has been following the terms of the contract, it may help the organization avoid fines for non-compliance and protect itself in case of legal action by its business partner or by the patients affected by the breach.

HIPAA (and your BA Agreements) will require your organization to put in place three kinds of safeguards for PHI:

- **Administrative.** This includes doing a risk analysis to understand what kinds of PHI you have, how you use it, where it could be vulnerable, and what the impact could be if it were lost, stolen, or exposed. Based on a risk analysis, you will develop policies and procedures to protect that PHI and to outline your response in case of a breach or suspected breach.
- **Technical.** These are safeguards built into your IT systems and procedures—even the ones you may have outsourced to another vendor such as an application services or network services provider. (Remember that the safeguards may include BA Agreements between you and those providers.)
- **Physical.** These include measures such as limiting access to your facilities, systems, and data storage areas to authorized personnel; having security policies for use of laptops and mobile devices; and making sure that materials are recovered and access is taken away when someone leaves your organization.

If you are a small or mid-sized organization, as are many BAs, chances are you don't have data privacy or security experts on staff, and starting on all these measures may be daunting. The best place to start is with the risk analysis. The results will show you where you are most vulnerable and where to concentrate your efforts and your spending. Guided by the risks, you can address the most critical areas first and then grow your security programs as necessity dictates and as time and budget allow.

PHI security is a lot to take on, especially in this age of cyberattacks and daily breaches. While it takes resources to put BA Agreements and new security and privacy procedures in place, in the end, they will benefit your business, your business partners, and the patients you both serve.

This article was posted on Healthcare IT News on June 23, 2015 at:
http://www.healthcareitnews.com/blog/how-succeed-hipaa-business-associate