Don’t be a HIPAA Lawbreaker

HIPAA Compliance Deadline Coming Fast

By Mike Semel

Facts:

- **HIPAA is a pain.**
- **HIPAA is expensive.**
- **HIPAA is the LAW.**
- **HIPAA requires that Business Associates comply by September 23.**
- **You now have risks with companies you may not even know exist.**
- **Breaking the HIPAA law can cost you your trust, your reputation, your customers, your career, and a lot of money. Two recent class action lawsuits from patients whose data was breached total $ 5.9 billion. Yes, *Billion*.**
- **Medical practices may lose their Meaningful Use incentive money.**

Is HIPAA really worth becoming a law breaker?

ANY PROTECTED DATA MANAGED BY OR SENT TO A NON-COMPLIANT IT SOLUTIONS PROVIDER, DATA CENTER, ONLINE BACKUP PROVIDER, OR CLOUD SERVICE AFTER SEPTEMBER 23 WILL BE A DATA BREACH THAT MUST BE REPORTED TO PATIENTS AND THE GOVERNMENT HIPAA ENFORCERS.

Data breach investigations often result in big fines and penalties for Willful Neglect— not making an effort to comply with HIPAA. Make sure your IT partners not only sign Business Associate Agreements, but really prove their compliance, and their subcontractors’, to you.

Think of all the work it took to get where you are. Think of all the time, effort, and money it took to get your organization where it is today. Now imagine that a HIPAA audit or data breach investigation results in a million-dollar fine and public humiliation. What if your medical practice or hospital loses your Meaningful Use incentive money? If you are the CEO or Practice Manager, do you want your name spread across newspapers, industry publications, and websites?

At a recent technology conference that included IT solution providers and their vendors, many companies showed that they did not understand the requirements, underestimated what needs to be done in less than two months before enforcement begins; or just don’t care that they are placing their customers at risk.

When asked if their companies were going to comply by the September 23 enforcement deadline…

> Some do not think anyone will care that sending them protected data will be a data breach that could cost millions of dollars. They think their business partners are either clueless or do not care that they have a legal obligation to comply.

Some said their lawyers were going to have Business Associate Agreements (BAA) ready prior to the deadline. However, when told that a BAA is only a paperwork component, they said they did not realize that they needed to implement a complete HIPAA compliance program, including a HIPAA risk analysis; HIPAA policies and procedures; completing employee HIPAA training; changing current processes and sometimes rewriting software to comply with HIPAA; and developing documentation to show compliance in the event of an audit. They originally had six months to comply. Some have not even started with just over six weeks to go.

Some said their companies "were working on HIPAA compliance" but could not offer any details. Scary.

HIPAA isn't New

HIPAA was passed by Congress in 1996. The Privacy Rule (2003) protected all patient data—verbal, written, and electronic. The Security Rule (2005) provided a security framework to protect electronic patient data. The rules defined health care providers and payers as Covered Entities. It defined businesses that support Covered Entities and had access to patient data as Business Associates. Covered Entities were required to comply or pay fines. Business Associates were out of reach of the HIPAA enforcers until the HITECH Act – in 2009— said that Business Associates would be directly liable for penalties.

Enforcement

The Security Rule (2005) was confusing to many health care organizations, and some ignored it completely. Because of funding limitations, the federal government was not enforcing HIPAA, so practices got away with non-compliance.

Over time it became apparent that Business Associates were responsible for many data breaches. When Congress funded Electronic Health Record incentives for doctors and hospitals in 2009, it also required Business Associates to comply and be directly liable for violations. Enforcement was funded and the enforcers were given financial incentives to be aggressive. (The first thing the enforcement agency did with the money was to hire a federal prosecutor as its new director.)

New Rules

The HIPAA Omnibus Final Rule, released in January, 2013, requires Business Associates to be responsible for their Subcontractors, and any Subcontractors they use. The rule also specifies that organizations that 'maintain' data, *even if they do not access it*, are Business Associates. This definition clearly includes data centers, online backup companies, and Cloud services that include any data storage. Examples include hosted Electronic Health Record (EHR) systems, e-mail providers, e-mail archivers, e-mail encryption services, file sync services, data backup and disaster recovery, and more. Business Associates were given until September 23 to comply before enforcement begins.

Compliance Requirements – More than Written Agreements

Just like Covered Entities, Business Associates must now not only sign Business Associate Agreements, but also implement full compliance programs.

Some software vendors and Cloud service providers have had to write programming code to comply with the HIPAA requirement for six years of data log retention. Some are changing their processes to manage hard disk drives. Some are having trouble getting their data centers to agree to HIPAA compliance. Time is up if you have to change vendors or move your equipment to another data center before the deadline.

Don't wait. What You Should Do Now?

Just because Business Associates have to comply does not mean a Covered Entity's risk has been reduced. In fact, because of the new requirements you are responsible for the compliance of any Subcontractors that work with your Business Associates, and you may not know who they are.

If you are a medical practice, get solid assurances that your IT service providers have signed Business Associate Agreements. More important than a signed piece of paper, make sure they understand HIPAA and have implemented compliance programs that will sustain an audit or data breach investigation. Make sure that they understand that they are responsible for their Subcontractors, who are responsible for their Subcontractors.

Ask if your data is backed up to an online vendor; if your EHR or e-mail is hosted or archived in the Cloud; if your servers are collocated in a data center, and make sure every vendor will sign a Business Associate Agreement and has implemented a real HIPAA compliance program. Be sure that every company that services your computers and copiers has signed a BA agreement with you or their resellers. Without good assurances, you should be VERY scared and replace these vendors so you don't have a data breach.

If you are an IT solutions provider, make sure your vendors and their vendors have signed Business Associate Agreements and that you are totally confident they have implemented real HIPAA compliance programs. If you aren't confident, remember that sending them data or having them repair a computer or server might be a reportable data breach. Protect your business, your customers, and your career. Move your business to a company that is in compliance.

Here is what a good Business Associate looks like:

- Business associate has been independently audited across all 54 HIPAA citations and 136 audited components; they've passed with 100% compliance and can show you a copy of their report.
- They can tell you the particular technologies they'll use to meet HIPAA security standards.
- They have documented policies and procedures already in place, including policies related to breach notification.
- They have proof their employees are trained on how to handle your PHI, with last completed dates of training.
- They should have their own business associate agreement in place that defines their responsibilities when handling your PHI.

Source: OnlineTech

Semel Consulting can evaluate the compliance efforts of your vendors. Recommend our compliance evaluations and remediation programs. We have over 10 years' experience with HIPAA, conducting assessments and remediation projects for doctors, hospitals, labs, and technology companies. Our lead consultant has been a hospital Chief Information Officer, owned an IT Solutions Provider, been the Chief Operating Officer for an online backup company, authored HIPAA training, and is a recognized authority on healthcare technology. Visit www.semelconsulting.com and read our articles at www.4medapproved.com/hitsecurity.

Mike Semel is a certified HIPAA expert with over 10 years' HIPAA experience and 30 years in IT. He has been the CIO for a hospital; owned and managed IT solution providers; ran operations at an online backup provider; and is recognized as a HIPAA thought leader. Contact Semel Consulting for more info.