Business Associates are NOT Responsible for Your Clients' HIPAA Compliance, *BUT You Still Might Be At-Risk*

By Mike Semel

"Am I responsible for my client's HIPAA compliance?"

"What if I tell my client to fix their compliance gaps, and they don't? Am I liable?"

"I told a client to replace the free cable Internet router with a real firewall to protect his medical practice, but the doctor just won't spend the money. Can I get in trouble?"

"We are a cloud service provider. Can we be blamed for what our clients do when using our platform?"

"I went to a conference and a speaker said that Business Associates were going to be held responsible for their clients' compliance. Is this true???"

I hear questions like these all the time from HIPAA Business Associates.

The answers are No, No, No, No, and No.

"A business associate is not liable, or required to monitor the activities of covered entities under HIPAA, but a BA has similar responsibilities as a covered entity with respect to any of its downstream subcontractors that are also BA's," said Deven McGraw, Deputy Director for Health Information Privacy, US Department of Health and Human Services Office for Civil Rights (OCR), Chief Privacy Officer for the Office of the National Coordinator for Health Information Technology. on August 17, 2017.

So, while you aren't responsible for your clients' HIPAA compliance, what they do (or don't do) still might cost you a lot, if you aren't careful.

In my book, *How to Avoid HIPAA Headaches*, there are stories about HIPAA Covered Entities that suffered when their Business Associates failed to protect PHI. North Memorial Health Care paid $ 1.55 million in HIPAA penalties based on an investigation into the loss of an unencrypted laptop by one of its Business Associates, Accretive Health.

Cottage Health, a California healthcare provider, is being sued by its insurance company to get $ 4.1 million back from a settlement after Cottage Health's IT vendor, a Business Associate, accidently published patient records to the Internet.

Your marketing activities; what you and your salespeople say to prospects and clients; and your written Terms & Conditions; may all create liability and financial risks for you. These must be avoided.

Semel Consulting works with a lot of Business Associates.

Many are IT companies, because I spent over 30 years owning my own IT companies. I've been the Chief Information Officer for a hospital and a K-12 school district, and the Chief Operating Officer for a cloud backup company. I now lead a consulting company that helps clients address their risks related to regulatory compliance, cyber security, and disaster preparedness. I speak at conferences, do webinars, and work with IT companies that refer their clients to us.

I look at the world through risk glasses. What risks do our clients have? How can I eliminate them, minimize them, or share them? When we work with our healthcare and technology industry clients, we help you identify your risks, and quantify them, so you know what resources you should reasonably allocate to protect your finances and reputation.

Under HIPAA, compliance responsibility runs one way – downhill.

Imagine a patient on top of a hill. Their doctor is below the patient. You are the doctor's IT support company, below the doctor, and any vendors or subcontractors you work with are below you.

The doctor commits to the patient that he or she will secure the patient's Protected Health Information (PHI) in all forms – verbal, written, or electronic. This is explained in the Notice of Privacy Practices (NPP) that the doctor gives to patients.

Under HIPAA, the doctor is allowed to hire vendors to help them do things they don't want to do for themselves. Vendors can provide a wide variety of services, like IT support; paper shredding; consulting; malpractice defense; accounting; etc. The patient is not required to approve Business Associates, and does not have to know that outsourcing is happening. This flexibility is also explained in the patient's Notice of Privacy Practices.

As a vendor that comes in contact with PHI, or the systems that house it, you are a HIPAA Business Associate. This requires you to sign Business Associate Agreements and, since 2013, when the HIPAA Omnibus Final Rule went into effect, it also means that you must implement a complete HIPAA compliance program and be liable for any breaches you cause.

IT companies may decide to resell cloud services, online backup solutions, or store servers in a secure data center. Since the HIPAA Omnibus Final Rule went into effect, a Business Associate's vendors (known as subcontractors) must also sign Business Associate Agreements with their customers, and implement complete HIPAA compliance programs.

Because compliance responsibility runs downhill, the doctor is responsible to the patient that his Business Associates will protect the patient's confidential information. The Business Associates assures the doctor that they, and their subcontractors, will protect the patient's confidential information. Subcontractors must commit to Business Associates that they will protect the information. A series of two-party agreements are required down the line from the doctor to the subcontractors.

It doesn't work the other way. Subcontractors are not responsible for Business Associates, and Business Associates are not responsible for Covered Entities, like doctors.

HIPAA compliance responsibility, and legal and financial liability, are different.

A HIPAA Covered Entity is responsible for selecting compliant vendors. Business Associates are responsible for selecting compliant subcontractors. Subcontractors must work with compliant subcontractors.

Because Covered Entities are not liable for their Business Associates, and Business Associates are not liable for their Subcontractors, they are not required to monitor their activities. But, you still need to be sure your vendors aren't creating risks. The Office for Civil Rights (OCR) says that:

> ***… if a covered entity finds out about a material breach or violation of the contract by the business associate, it must take reasonable steps to cure the breach or end the violation, and, if unsuccessful, terminate the contract with the business associate. If termination is not feasible (e.g., where there are no other viable business alternatives for the covered entity), the covered entity must report the problem to the Department of Health and Human Services Office for Civil Rights. See 45 CFR 164.504(e)(1).***
>
> ***With respect to business associates, a covered entity is considered to be out of compliance with the Privacy Rule if it fails to take the steps described above. If a covered entity is out of compliance with the Privacy Rule because of its failure to take these steps, further disclosures of protected health information to the business associate are not permitted.***

In its Cloud Service Provider (CSP) HIPAA Guidance released in 2016, the OCR said:

> ***A covered entity (or business associate) that engages a CSP should understand the cloud computing environment or solution offered by a particular CSP so that the covered entity (or business associate) can appropriately conduct its own risk analysis and establish risk management policies, as well as enter into appropriate BAAs. See 45 CFR §§ 164.308(a)(1)(ii)(A); 164.308(a)(1)(ii)(B); and 164.502.***
>
> ***Both covered entities and business associates must conduct risk analyses to identify and assess potential threats and vulnerabilities to the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit. For example, while a covered entity or business associate may use cloud-based services of any configuration (public, hybrid, private, etc.),[3] provided it enters into a BAA with the CSP, the type of cloud configuration to be used may affect the risk analysis and risk management plans of all parties and the resultant provisions of the BAA.***

How can a Business Associate be affected by a client's compliance failure? Here are some scenario's.

(FYI, I am not a lawyer and this is not legal advice. These ideas came out of meetings I had with my attorney to review our contracts and our marketing. Talk to your lawyer to make sure you are protected!)

1. **IT companies should never tell your client, "We'll be <u>responsible</u> for your IT so you can focus on your medical practice."**

   Sound familiar? This is what many IT Managed Service Providers tell their prospects and clients.

   Then the client has a data breach because they were too cheap to buy a firewall, they refused to let you implement secure passwords because it would inconvenience their staff, or they lost an unencrypted thumb drive even though you had set up a secure file sharing platform.

   Someone files a HIPAA complaint, the OCR conducts an investigation, and your client pays a big fine. Then they sue you, saying you told them IT was your responsibility. Maybe they misunderstood what you included in your Managed Services. Maybe you did not clearly explain what responsibility you were accepting, and what IT responsibility was still theirs. Either way, you could spend a lot on legal fees, and even lose a lawsuit if a jury believes you made the client believe you were taking over their compliance responsibility.

2. **You must clearly identify what is, and what is not, included in your services.**

   Your client pays you a monthly fee for your services. Then they have a breach. They may expect that all the tasks you perform, and the many hours of extra labor you incur, are included in their monthly fee. They get mad when

you say you will be charging them for additional services, even though they have just hired a lawyer at $ 500 per hour to advise them. Without written guidelines, you may not be able to get paid.

3. **You must be sure you get paid if your client drags you into something that is not your fault.**

   Imagine you were the IT company that set up an e-mail server for a recent presidential candidate. As unlikely as this may sound, this becomes a political issue. You just did what the client requested, but now you must hire attorneys to advise you. You must hire a public relations firm to deal with the media inquiries and protect your name in the marketplace. You must send your techs and engineers – your major source of a lot of income – to Washington for days to testify in front of Congress, after they spent more unbillable time preparing their testimony.

   Who pays? How do you keep from losing your client? How do you protect your reputation?

HOW TO PROTECT YOUR FINANCES AND YOUR REPUTATION

- Make sure you and your salespeople are careful to not overpromise your services. Make sure you and your sales team tell your prospects and clients that they are always ultimately responsible for their own security and compliance.

- Make sure your contracts and Terms and Conditions properly protect you by identifying what services are/aren't covered, and when you can bill for additional services. Don't forget to include your management time when sending bills. Use a competent lawyer familiar with your needs to write your agreements and advise you on any agreements presented to you by others.

- State in your Terms & Conditions that you will be responsible for your own company's compliance (you are anyway) but that you are not responsible for your clients' compliance.

- Include terms that require your client to pay for ALL costs related to a compliance violation, government action, investigation, lawsuit, or other activity brought against them, that requires your involvement. Use a competent lawyer familiar with your needs to write your agreements and advise you on any agreements presented to you by others.

- My attorney said we should include "change in government regulations" in our Force Majeure clause to allow us to modify our contract or our pricing before a contract expires. The 2013 HIPAA Omnibus Rule created a lot of expensive responsibilities for Business Associates. You don't want to get stuck in an existing contract or price model if your costs suddenly increase because of a new law or rule.

- Get good Professional Liability or Errors & Omissions insurance to protect you if you make a mistake, are sued, or dragged into a client's investigation. Make sure you understand the terms of the policy and how it covers you. Make sure it includes legal representation. Ask for a custom policy if you need special coverage.

- Make a negative a positive by promoting that you offer the specialized services clients will need in case they are ever audited, investigated, or sued.

If you do this right, you will protect your business and leverage compliance to increase your profits. When you focus on compliance, you can get clients willing to pay higher prices because you understand their compliance requirements. I know. I have generated millions of dollars in revenue using compliance as a differentiator.

###

Mike Semel Bio

Mike Semel is a noted thought leader, speaker, blogger, and best-selling author. He is the President and Chief Security Officer of Semel Consulting, focused on HIPAA (and other regulatory) compliance; cyber security; and Business Continuity planning. Mike is a Certified Business Continuity Professional through the Disaster Recovery Institute, a Certified HIPAA Professional, Certified Security Compliance Specialist, and Certified Health IT Specialist. He has owned or managed technology companies for over 30 years; served as Chief Information Officer (CIO) for a hospital and a K-12 school district; and managed operations at an online backup company.