EMR & HIPAA
Powered by HealthcareScene.com

HIPAA May be the Least of Your Compliance Worries

What requirements have you hidden away?

I visited a new healthcare client last week, and asked if anything in particular made them call us for help with their HIPAA compliance. They surprised me by saying that their insurance company had refused to sell them a cyber-liability/data breach insurance policy, after they saw the answers on our client's application.

When was the last time you heard about an insurance company *not* selling a policy? That's like McDonalds looking you over, and then refusing to sell you a Big Mac.

Our client was scared that they would have to risk the full financial burden of a data breach, which, based on the number of medical records they have, could exceed $ 10 million.

Everyone knows that HIPAA is a compliance requirement. But it isn't the only one you should focus on. Use my definition of Compliance, which is, simply, ***having to do things required by OTHERS***.

We personally deal with compliance requirements all the time. We stop at traffic lights. We have our car inspected. We fasten our seat belts. We empty our pockets at airport security. We pay our bills on time. At work, we wear an ID badge, show up on time, and park in an approved space. At home, we take our dirty shoes off before walking on the carpet. There are risks associated with NOT doing each of these things.

It can be a big mistake to focus so much on HIPAA that you forget other compliance requirements, including:

- Other Federal and State Laws
- Industry Requirements
- License Requirements
- Contractual Obligations
- Insurance Requirements
- Lawsuits

You should not take the narrow HIPAA approach, like buying a policy manual, using an online 'We Make HIPAA Easy' service, or think hiring out a Security Risk Analysis is going to make you compliant.

When we work with our clients, before we get started we help you identify all your compliance requirements.

OTHER FEDERAL REGULATIONS

Depending on the services you offer, you may be required to comply with other federal regulations, like Title 42, governing substance abuse treatment.

The Federal Trade Commission has come down hard on data breaches, including the controversial closure of a small medical lab. The FTC looks at patients as consumers, and considers a data breach to be an Unfair Business Practice because the organization losing the data failed to protect its consumers, and is in violation of its Notice of Privacy Practices.

STATE LAWS
Forty-eight states, plus DC and Puerto Rico, have data breach laws. Most states protect Personally Identifiable Information (PII), including driver's license and Social Security numbers. Some states cover medical records, no matter who has them, while HIPAA only covers medical records held by certain types of organizations. Some of the state laws change the reporting requirements after a breach of patient records. For example, California requires patient notification within 15 days, instead of the 60-day maximum permitted by HIPAA.

Most states have separate laws requiring confidentiality of mental health, HIV, substance abuse, or STD treatment records. State attorneys general are willing to cross their state lines to protect the confidentiality of their voters.

We work with our clients to identify the states where your patients come from, not only where you are located. We build an Incident Management program that includes each applicable notification and reporting requirement.

INDUSTRY REQUIREMENTS
Industry requirements include PCI-DSS, the data security standards protecting credit card information. PCI stands for the Payment Card Industry. While not a law, if you don't comply with PCI you can be prevented from accepting credit cards. What would that do to your bottom line and patient satisfaction?

LICENSING
Licensing requirements protecting patient confidentiality go back long before HIPAA, which became law in 1996. In 1977, 19 years before HIPAA, I became an Emergency Medical Technician (EMT). The first class I took was about maintaining confidentiality. After that, I knew that violating a patient's confidentiality could cost me my license.

Think about your license, your certifications, even the Code of Ethics in your professional association. If I really wanted to get back at someone for violating my confidentiality, my first complaint would be to their licensing board, even before I submitted a complaint to their employer or the federal government. Losing your license may kill your career, and being investigated by your licensing board will certainly get your attention.

When you are justifying the costs related to Security and Compliance, be sure to quantify the effect on your income, lifestyle, and retirement, if you were to lose your license.

CONTRACTS
Many of our clients have signed contracts with other organizations, that include cyber security requirements as a contractual obligation to do business together. These contracts are often reviewed by attorneys, signed by executives, and then filed away. The requirements are not always communicated to the people on the front lines.

In 2012, Omnicell, a drug cart manufacturer, breached the records of 68,000 patients when an employee's unencrypted laptop was stolen. The health systems - clients of Omnicell - announced that Omnicell's contract with them included a requirement that patient data would only be stored on encrypted devices. The loss of the laptop became a breach of contract discussion, not just a simple data breach.

My guess is that the contract was signed, and then just filed away. I don't think Omnicell's purchasing department was told it was supposed to order encrypted laptops for its field technicians. I don't think its IT department knew it had a contractual obligation to install encryption on all laptops, and I doubt the field tech

knew he was violating a contract when he transferred patient data to his unencrypted computer. Worse, no one who was aware of the contract requirements was auditing the company's compliance.

During a recent client visit, I asked if our client had signed any contracts with their clients. She went through a list that included one of the top health systems in the country. I'm not a lawyer, but I asked to see the contract, because I knew the health system had included cyber security requirements as a contractual obligation with our other clients.

After a few minutes, she returned with the file folder containing the contract. I found the cyber security section, and read it to her. I asked if her company was meeting the requirements in the contract. She said no. I asked her what the future of her business would look like if they lost the business of one of the country's leading health systems, because they breached their contract. She replied that her business probably would not survive.

We focused our project around meeting the specific requirements of their contract, not the vague and flexible requirements in HIPAA.

INSURANCE

Cyber Liability (also known as Data Breach) Insurance is a popular line of revenue for insurance companies. Unlike malpractice insurance, which assumes you will make a mistake, cyber insurance may only protect you if you are doing all the things you included on your insurance application. It may pay a claim only if you are doing everything correctly, and still suffer a breach. What you answer on the application may come back to haunt you.

In 2013, Cottage Health's IT vendor accidently published a file server to the Internet, exposing patient information. Patients Googling themselves got back their medical records. The patients filed a class action suit, so Cottage Health brought in Columbia Casualty, their cyber liability insurance provider, to provide legal representation, and settle the claim.

The lawsuit was settled for $ 4.1 million, which was paid by Columbia Casualty. Columbia told Cottage Health that, even though it was making the payment, it still reserved its rights and would continue investigating the case.

Columbia Casualty then sued its own client, Cottage Health, to get the $ 4.1 million back. It said it determined that Cottage Health had made misstatements when it answered questions on the original policy application, including that it regularly maintained security patches on its devices. Columbia also said it should be excluded from losses because Cottage Health failed to continuously maintain the level of security stated on its application.

The lawsuit said that it did not matter if Cottage Health was mistaken, or had intentionally lied on the application.

As part of our assessments, we review insurance applications. When we work with our clients, we help you implement consistent programs to maintain the level of security you claim on your application.

LAWSUITS

While you don't comply with a lawsuit, watching court cases can help you understand your risks and how to protect your organization.

Many people think that a HIPAA Notice of Privacy Practices is just a basic brochure you have to include with new patient paperwork. A patient is suing her doctor for negligence after her information was shared without her authorization. She claimed that the practice did not follow its Notice of Privacy Practices, and the Connecticut Supreme Court upheld that HIPAA can be used as a Standard of Care in a negligence suit.

Walgreen's lost $ 1.44 million in a lawsuit after a pharmacist breached a customer's confidentiality. Walgreens proved its pharmacist had received HIPAA training and had signed a confidentiality agreement. The company said it had done everything possible to prevent the breach. The jury disagreed.

By looking at law suits you can see that attorneys are using compliance requirements as the basis for claims. That can be scarier compared to the likelihood is that the federal government will make the effort to go after you.

LESSONS LEARNED

It's really easy to focus just on HIPAA and think you are compliant. It's also a mistake.

HIPAA is vague. It is flexible, giving you a lot of freedom to choose how to comply with the regulation. The 'HIPAA-in-a-Box' solutions can give you a false sense of Security and Compliance, because they are so narrowly focused.

The Federal Trade Commission can assess stronger penalties than the OCR, the federal agency that enforces HIPAA. The FTC has put businesses on 20-year monitored compliance programs. When we work with our clients, we help you create written evidence that your security policies and procedures are working.

State laws can change your patient reporting requirements. They also protect confidential information you have for your workforce members. Your Incident Management program can't just focus on HIPAA.

Industry requirements can be very serious. Can you risk not accepting credit cards? Contact the merchant service that processes your cards to make sure you are complying with PCI-DSS.

Verify the reporting requirements of the entities that license your staff. You may have an obligation to report a breach to them, instead of waiting for someone to file a complaint.

Review the contracts you have in your files for cyber security requirements, and note any in new contracts you are about to sign. Make sure everyone in your organization who must comply with the contract requirements know about them.

You can't buy insurance instead of doing the right things to protect data. However, if you do things right insurance may save you millions of dollars. You should review your policy application every quarter, and demand evidence from your IT department or vendor that you are in compliance with the policy requirements. Too much work? Would you rather have your insurance company fail to pay a multi-million-dollar claim?

Keep repeating to yourself, "Compliance isn't just about HIPAA" and uncover the rest of your compliance requirements.

###

About Mike Semel

Mike Semel is a noted thought leader, speaker, blogger, and best-selling author of HOW TO AVOID HIPAA HEADACHES . He is the President and Chief Security Officer of Semel Consulting, focused on HIPAA and other compliance requirements; 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.