Clearing Up the Confusion Between Security, Privacy, HIPAA and HITECH: An Interview With Steve Spearman

Mary Pat: Your business is called "Health Security Solutions." People often confuse privacy with security. Can you clear up the confusion for us?

Steve: The Privacy rules refer to the broad requirements to protect the confidentiality of Protected Health Information (PHI) in all its forms. So for example, a physician talking loudly on the phone in the lobby of a restaurant about a patient by name is a violation of the privacy rules. **PHI on paper records is covered under the privacy rules.**

The security rules are specifically concerned about protecting the confidentiality (i.e. privacy), integrity and availability of electronic PHI, or PHI that exists in a digital form. So once you are dealing with **electronic health records and information systems, violations tend to fall under the security rules.**

Let me illustrate with an example. A traditional fax machine is generally considered under the rules to be an analog device. So if a practice takes a patient face sheet and faxes it to another another practice who also has a traditional line to line fax machine, it would fall under the privacy rules. However, if one practice has a traditional fax machine and is faxing the document to a practice that has either a fax server or a fax service (like eFax), then the data is digitized before it is processed on the receiving end. That second practice's fax would be covered under the security rules

because the data is digitized.

Mary Pat: Okay, that helps a lot. The difference between HITECH and HIPAA can also be confusing – can you clarify?

Steve: That's a great question. **HIPAA** defines the rules related to the privacy and security of patient health information and has been around since 1996 with periodic updates since then.

HITECH is a subsection of the American Recovery and Reinvestment Act (ARRA) legislation that provided incentives to physicians and hospitals to "meaningfully" adopt EHR solutions. But the act also contained elements related to the security of ePHI. Specifically, it clarified and strengthened the law as it pertains to business associates. Prior to HITECH, the liability of Business Associates (BAs) was mostly limited to breach of contract under the terms laid out in a business associates agreement. HITECH clarified that Business Associates were required to comply with all the HIPAA requirements and dramatically strengthened enforcement by specifying that the increased fine levels, up to $1.5M, applied to BAs as well as covered entities. Probably the most significant security related provision of the HITECH Act was the Breach Notification requirement. Under that requirement, covered entities and business associates are required to report to DHHS any unauthorized breach of PHI unless the data was secured through encryption.

As you may have heard, the Omnibus HIPAA regulations were just published and will go into effect in a couple of months. One of the objectives of the rules is to consolidate the HITECH security related provisions under the HIPAA umbrella. So when the laws take effect, those security provisions that were a part of HITECH will be covered under the HIPAA mandates.

Mary Pat: Many practices are overwhelmed with trying to meet all the federal program mandates and keep up with all the

other changes. What are two things that all practices should be doing right now to become compliant with the law and protect their practices?

Steve: I am tempted to give an overly long answer to this question. But I'll try to keep it simple. **One, the practices need to have the required set of security and privacy policies in place.** Most practices have some or many privacy policies in place but, based on my experience, are missing the security policies. For example, every practice has to have the following policies and procedures:

- a sanction policy
- a named security officer,
- an information system activity review an audit procedure, and many more.

A good set of template policies can set you well on your way towards compliance. ***(If you contact me, I am happy to talk to anyone about places they can go to get security policies including a set of free policies that I have recently reviewed)***. Any covered entity with a breach of ePHI that is found to have been willfully neglectful will face heavy fines (as high as $1.5M). Policies and procedures are a first good step to avoid the willful neglect designation.

Two, at the risk of sounding self-serving, they need to protect the ePHI that they are creating, transmitting or storing. And a risk analysis is the first step to that process. It is also the first and a required HIPAA Security safeguard. For most clinics, there tends to be a fairly predictable set of vulnerabilities that they need to address but every practice is different and the risk analysis helps you get to the bottom of these.

Mary Pat: Do small practices have less to worry about as far as security than large practices?

Steve: They don't have less to worry from a compliance

standpoint. They have to abide by the HIPAA rules to the same degree as large practices. However, there are elements within the rules that allow for latitude based on the resources and complexity of organizations. So I might advise an 18-physician orthopedic practice that they need to implement a security measure that I would not advise a smaller practice to implement. In a smaller practice setting, for example, all the employees know each other. So if some unknown person is attempting to get into the data closet, someone will notice and stop them. Although the data closet should be locked in most practices of any size, in a large practice or enterprise it should be alarmed and monitored as well. Although larger practices tend to have more resources at their disposal, in many ways it is easier to get a small clinic into compliance.

Mary Pat: Does using a cloud-based practice management or electronic medical record system alleviate security requirements, or does it make the security requirements more stringent?

This is a controversial opinion but, on net, I think that cloud-based, hosted and Software as a Service (SaaS) solutions make compliance easier. I have two main reasons for that assertion. I believe that a large breach involving multiple records is less likely. The physical security of the server is invariably much, much better with hosted solutions. These solutions are often deployed in SSAE 16 certified data centers which require extremely rigorous security practices. In addition, they are frequently deployed using either a virtual environment or terminal services which means that data is not being stored or cached on the desktop or laptops. **Remember, about 80% of the reported breaches involve stolen laptops and other "client" devices**. Another benefit of SaaS solutions is that they often do much of the heavy lifting related to contingency planning and data backup.

There are some negative trade-offs. Many service agreements with SaaS providers are wholly inadequate. The contract with a

service provider should state clearly that the covered entity owns the data. They should also document a procedure to provide at zero or very minimal cost an exact copy of the ePHI owned by the covered entity in the event that the service provider goes bankrupt or the provider just wants to cancel its contract. The procedure for this transfer of data needs to be spelled out in the service agreement and/or in the practice's contingency plan. And, ideally, it needs to be tested periodically. In addition, I have a concern that many solution providers are unaware that they are bound by all the HIPAA regulations and don't take sufficient precautions in safeguarding their data. Some solution providers do better than others. Another concern, that is becoming less and less true over time, is that access to the record is dependent on a persistent internet connection. Since protecting the "availability" of ePHI is one of the goals of the regulations, dependence on an internet connection makes a compromise in this area a bit more likely. Contingency plans need to address this concern and a redundant connection should be a part of that.

I would finish by pointing out that solution providers can "scale" and can not only afford but have the incentives to invest in security infrastructure and expertise. A hosting provider can afford to hire someone with a Masters in Information Security or with the CISSP certification while the typical practice cannot. Although HIPAA has many components and I have concerns about hosted solutions, the event that will land a provider in the news is a breach involving 100's of records and, based on my experience, this is less likely to happen with a service provider.

Mary Pat: Are HIPAA violations more likely to happen with larger practices, or are larger practices more likely to self-report?

Steve: I honestly don't have a good bead on that. If by "HIPAA violations", you mean unauthorized disclosure of PHI, then I

would guess it mimics pretty well the demographics. In other words, the percentage of violations in large practices roughly approximates the percentage of physicians in large practices. Larger practices seem to do a better job at having incident reporting and response procedures in place and, if this is true, they would be more likely to self-report. But I'm just guessing.

Mary Pat: What importance does the new HIPAA Omnibus Rule have for medical practices?

Steve: I partially covered this in my earlier response. The most significant change is to the breach notification rules. The new rules replace the "no harm" standard with a "probability that data was compromised" standard. The "no harm" standard does not require improper disclosure of protected health information (PHI) to be reported as a "breach" unless "significant risk of financial, reputational, or other harm to the individual" whose data was exposed. This regulation was overturned for being too subjective. According to the new standard, an improper disclosure does not need to be treated as a breach if the covered entity can demonstrate "that there is a low probability that the PHI in question has been compromised." I am not sure how much less subjective that is but I think it will make the need to report a breach more likely.

I have written a pretty extensive summary of the new laws on my blog in a three-part series. **Part One is here.**

Mary Pat: Can you explain what BYOD means and why it is a security concern in healthcare?

Steve: BYOD stands for Bring Your Own Device. It essentially describes the use of personally owned devices such as iPhones, iPads, Android phones and tablets. Enterprises are reluctant to buy these devices for all employees due to cost. However, their use has potential benefits for organizations but also

presents some security concerns. The class of devices normally associated with BYOD is mobile devices which are generally a higher security concern due to the risk of theft or loss. However, that risk is increased with personally owned devices because organizations don't have the "control of ownership." If I am your employer and I hand you your own laptop, you won't think twice if I tell you, "here are the rules about what you can and can't do with that laptop." That ability to make rules, manage behavior and apply technical controls is much easier and clearer when an organization owns a device. It's harder if you don't. However, regardless of who owns a device, that control is essential! The only way BYOD can work from a security standpoint is if management can dictate the rules and controls for the use of personally owned devices. So a physician who wants to use his own iPad should be required to abide by all the policies of the organization such as limiting what applications can be installed, requiring a good complex password, enabling encryption, enabling auto-wipe in the event of multiple unsuccessful logon attempts, etc. There is a type of software called Mobile Device Management that can help enterprises with this effort. In the case of iOS devices, Apple has published some great resources to help companies with this effort which can be found **here.**

Mary Pat: I see that you offer free security tools on your website – what are they?

Steve: They are a hodge-podge of various tools and resources that I have gathered or developed that I have found to be particularly useful. My favorites are the security posters. (*In fact, for the first five readers of this interview that **fill out the contact form on my site here,** I will send full color, 11×17 versions of the "Seriously" and "Bad Links" posters in the mail for free!*) We have some new posters in development which we will be releasing soon. Although not in the free tools section of the website, I have gotten a lot of positive feedback on the Ten Steps to HIPAA compliance, which

goes along with one of my most popular presentations. I also really like the free tools from Sophos.

Mary Pat: What question(s) do you wish I had asked?

Steve: I have always wanted to be asked, “Why are you so devilishly handsome?” But it has yet to occur.

How about this question: Should practices outsource their meaningful use risk analysis or do it themselves?

My answer is multi-faceted. If the following two things are true, then it may make sense for a practice to do their own risk analysis. 1) You have access to some IT resources with at least some expertise in IT security and HIPAA. 2) Your objective is just to be able to attest in good faith to meaningful use and the actual security of your information systems is not really a big concern. I might advise a client where those two conditions are met to do their own risk analysis. Let me elaborate on them a bit. Many clinics outsource their IT to outside vendors. Occasionally those vendors are willing to make a meaningful commitment to understanding the risk analysis process as defined by NIST SP 800-30 and to understanding the HIPAA requirements. This is very unusual but not unheard of. In most cases though, IT vendors will readily acknowledge that they do not understand the requirements and are not comfortable being called on to fulfill them. In fact, one of the biggest sources for me of customers are these IT vendors that do not wish to take on the liability associated with HIPAA. Unfortunately, many practices assume that their IT vendor is meeting its HIPAA obligations. This is both unwise and unfair. If this is a practitioner’s expectation, then get it in writing. Adjust your service level agreement to reflect this fact. For most IT vendors though, they are going to charge the customer anyway for their compliance and training efforts.

In some cases, larger practices may have these resources

internally. The practice might have its own IT staff and someone could be assigned to the role of HIPAA security compliance and could be given the responsibility and resources to know and understand what needs to be done and to doing it. Large practices are the ones in which I am most likely to encourage an internally conducted risk analysis.

The point of #2 reflects the reality that many practices just want to be able to do enough to show a good faith effort that will allow them to receive their meaningful use check. Go through the process and assembling documentation to prove that a provider has conducted a risk analysis is not quite as hard as actually securing ePHI. I have conducted a half a dozen risk analysis for clients where I was doing a review or follow-up of a previous risk analysis. In every case, I was able to uncover medium to severe security risks that needed to be mitigated.

Even the Office of the National Coordinator, although clearly disclaiming that a risk analysis must be outsourced, encourages the risk analysis to be conducted by third parties. In its Guide to the Privacy and Security of HIT they state (p.17):

> ***Select a qualified professional to assist you with the security risk analysis. Your security risk analysis must be done well or you will lack the information necessary to effectively protect patient information. Note that doing the analysis in-house may require an upfront investment developing a staff member's knowledge of HIPAA and electronic information security issues. Use this opportunity to have your staff learn as much as possible about health information security.***
>
> ***You however, can conduct the risk analysis yourself. Just as you contract with professionals for accounting, taxes, and legal counsel, so, too, outsourcing the security risk analysis function can make sense….If you need to, outsource***

this to a professional; a qualified professional's expertise and focused attention will yield quicker and more reliable results than if your staff does it piecemeal over several months. The professional will suggest cost-effective ways to mitigate risks so you do not have to do the research yourself and evaluate options.

Steve Spearman, Founder and Chief Security Officer for Health Security Solutions, has been in the health care industry since 1991. After spending more than a decade observing health care providers struggle with the HIPAA Security and Privacy regulations, he founded Health Security Solutions in the summer of 2010 to help organizations minimize and mitigate the financial, legal, and compliance risks associated with running health care organizations.

Steve alongside his team of security experts, have helped healthcare providers qualify for millions of dollars worth of stimulus funding through a wide range of HIPAA consulting services and solutions, including his very own risk assessment method, **Risk Analysis in A Box**.

To learn more about Steve, Health Security Solutions, and the services they provide please visit **www.healthsecuritysolutions.com.**