Incorporating risk analysis into your HIPAA strategy

Author Name **Patrick Ouellette** | Date **May 8, 2014** |

In building a stout privacy and security compliance program that would stand up well to federal HIPAA audits, proactive healthcare organizations are generally rewarded when it comes to data breach avoidance and remediation. But an important piece of that equation is performing consistent risk analyses.

As Edward Zacharias, partner and a member of the Global Privacy and Data Protection Group at international law firm McDermott Will & Emery, detailed to *HealthITSecurity.com*, risk management is evolving with new technologies and organizations need to stay on top of potential threats. Read the Q&A with Zacharias below.

What types of HIPAA compliance trends are you seeing right now from healthcare organizations?

I think we're seeing, even though the HIPAA Omnibus Rule had been anticipated for a few years and most provisions became effective in September 2013, there is a continued focus on HIPAA compliance.

In particular, I think that a lot of the headlines are grabbing people's attention as well. Not just where the Office for Civil Rights (OCR) has announced enforcement actions, but just the sheer number of reported breaches. Where the trend is going, and where a company should be focused, is on being proactive rather than reactionary. Because what happens when an organization has one of these breaches, the enforcement authorities come in and, typically, the penalty isn't in response to the breach itself, it's more so the underlying actions (or lack thereof) that created the conditions for the breach to occur.

Why do most of these reported healthcare breaches tend to involve a missing laptop or thumb drive?

At a company level, it's a risk management issue. On one hand, you have this push across the healthcare spectrum for everything to become electronic and paperless for security, quality care and ease-of-access reasons. Hand-in-hand with that concept, as there's more laptops, tablets and smartphones with patient data potentially on them, I think [mobile strategy] needs to be part of the overall risk management approach. This includes taking inventory of the devices, where the information is stored and ensuring there are policies in place that address whether employees can use BYOD devices. I think what needs to happen, and what is happening on some levels, is a risk analysis of all the places that sensitive information comes in and out of the organization and address the security risks.

Are there some best practices that you can think of as an organization tries to "find its data"?

When organizations implement their policies and procedures, particularly on risk analysis, those documents should be pretty detailed about how and when it's going to be conducted. Depending on the size of the organization, sometimes it makes sense to even expressly include in that policy the specific members of the organization that are going to be responsible for the [risk analysis]. Certainly, you're going to want your IT folks involved because some of this can be esoteric on the technology front, you'll want your privacy specialists and perhaps a member of senior management involved as well.

How do your customers perceive cloud computing?

There are a few issues with cloud computing that are coming to the forefront [for healthcare organizations]. First, I think that with the rest of the IT world, cloud vendors are getting better at securing information and seems to be the direction that more organizations are going. The big piece of a provider's cloud environment is the availability of the information, as well as whether it's retrievable and able to be manipulated again to report quality metrics. There are a number of good reasons to implement cloud, but one of the things that organizations focus on as they move toward cloud computing is that data access.