FROM THE PODCAST PRODUCED BY

HEALTHCARE INFO SECURITY®

Asking BAs for Risk Management Proof

APRIO'S SCHROEDER DISCUSSES EVIDENCE HEALTHCARE ORGANIZATIONS SHOULD DEMAND

The following is a transcript of an interview with Dan Schroeder, partner-in-charge of Information Assurance Services with Aprio, by Marianne Kolbasuk McGee, executive editor of Information Security Management Group. The interview was published at http://www.healthcareinfosecurity.com on Dec. 16, 2015. It has been edited for clarity and conciseness.

When it comes to safeguarding patient data, what should covered entities demand from their business associates? In the following interview with HealthcareInfoSecurity, Aprio's Schroeder discusses the top questions covered entities (CEs) should ask their business associates (BAs) about security.

Marianne Kolbasuk McGee: When covered entities are considering working with a vendor that will handle protected health information, what are the most important questions that they should ask their BAs about security?

Dan Schroeder: The covered entity in today's environment needs to know that the business associate understands the risks that they represent to the CE; that they have an effective risk management program in place; and finally, that they can provide the appropriate form of evidence to the CE that those right things relative to risk management are deployed and operationally effective.

MKM: Under the HIPAA Omnibus Rule that went into effect in 2013, BAs are directly liable for HIPAA compliance. But the HIPAA Security Rule was written years ago before many of today's sophisticated cyber threats emerged. With that said, should CEs expect their BAs to go beyond the basic requirements of HIPAA requirements in safeguarding patient data?

DS: It is possible that there is some degree of risk management that is necessary that is over and above the Omnibus Rule and the HIPAA Security Rule. But for starters, there is a foundational element that would be the starting point of what the covered entity would need to know: Has the BA effectively completed a risk analysis as called for by the HIPAA Security Rule? Without an effective risk analysis, it is unlikely that the BA is going to know the right things to do for risk management and, finally, to be able to prove that. While the modern threats associated with cyber certainly are occurring well after when the Security Rule was written, it is very interesting that the Security Rule and the nature of the risk analysis still are very timely today. Risk analysis is the foundation, not just of HIPAA compliance, but also of cyber security risk management.

MKM: What kinds of assurance or evidence should covered entities expect from their BAs to ensure that the BAs are actually doing what they say they will be doing to protect patient data?

DS: One approach would be to obtain some form of an audit report or certification report from the BA and then to ensure that the report fulfills the requirements of the BA and provides the information necessary for the CE to be

comfortable that the right type of risk management program is in place. There are a couple of alternatives from the American Institute of Certified Public Accountants. SOC 1 (formerly known as SSAE 16) can be a great report for financial matters (for example, the processing of claims and management of financial assets), but it is a very poor report for privacy and security matters. An alternative AICPA report structure and standard known as SOC 2, when performed effectively to encompass security, privacy and (potentially) integrity, can be a great vehicle for communicating to the CE that the BA has properly understood the risks they represent to the CE, that they have defined an effective risk management program, that there is a set of testing over those controls, and to provide evidence back to the CE that those controls are deployed and operationally effective for some extended period of time.

Another alternative is HITRUST, with which many in the healthcare industry are familiar. The foundation of HITRUST is modeled after some of the more widely recognized security frameworks, including the NIST 800-53 standards put forward by the National Institute of Standards and Technology and ISO 27001. Many in the healthcare community like the HITRUST structure because it is tailored for security purposes in the healthcare setting. One option is that BAs can get a HITRUST certification from a certified HITRUST assessor. Recently the AICPA has, in conjunction with HITRUST, come up with a model whereby HITRUST also can be incorporated under SOC 2 reporting, so that a BA could produce an SOC 2 report that is extended so as to incorporate HITRUST criteria.

MKM: When you work with CEs and BAs, when it comes to their business associate agreements (BAAs), what do you see often overlooked or neglected that should be part of these agreements that would help with the assurance that the BA is actually going to do what the CE expects?

DS: I think this whole area associated with governance and risk management of vendors is something the healthcare industry struggles with, as do other industries. Whether it's part of the BAA or just ongoing vendor management, it comes down to having the right protocols in place for the CE to have complete assurance that the right things are happening from a risk management perspective. Too many times, a CE will see that a BA has some form of a report that purportedly addresses privacy and security related matters, and the CE might assume that the mere existence of that report is evidence that their risk management needs are represented. We know that, in many cases, that is not the case. And it's not necessarily something intentional on the part of the BA, where they are intending to deceive the CE. It is from a lack of understanding or confusion about what is in these reports. Whether it is part of the BAA or ongoing management or oversight of the vendor/business associate, first and foremost, CEs must get real proof that there is an effective risk management program, starting with an effective risk analysis that underlies and that is performed in the context of the services that the BA is performing for the CE. Then, can the BA provide evidence that they have aligned a risk treatment program in conjunction with that risk analysis? And finally, is there some kind of assurance report that the BA can give to the CE that would serve as some form of evidence that those right things are happening?

On the topic of assurance reporting, the CE will have to determine what level of assurance is necessary for them. In some cases, an assurance could be the word of an executive, perhaps in a letter, where they say, "You can trust us." In other cases where there is a high degree of risk relative to the confidentiality, integrity and availability of protected health information, that CE may want to have an independent assurance report performed under professional standards that provides a higher level of assurance so they can trust that the right things are happening from a BA. Our firm, in full disclosure, is not just a consulting firm. We are a CPA firm. We are part of the community that issues SOC 2 reports, which would be an example of the type of report that would be done under professional standards and that provides a higher level of assurance with respect to the nature of services being performed by the BA and the risk management program that is in place.

MKM: How about penetration testing? Often you hear that CEs are interested in seeing the results of penetration testing on the BA, but often there is pushback because that might be revealing too much about the vulnerabilities that a BA has. Where do you stand on that?

DS: Pen testing is an interesting topic. Our definition of penetration testing aligns to some of the formal definitions from the likes of the NIST. It is a manual and automated means of identifying vulnerabilities, as well as the exploitation of those vulnerabilities for the purpose of confirming that the vulnerabilities can be exploited and that information assets can be compromised. It involves trained, skilled individuals attempting to perform ethical hacking to get into a system to see if they can actually find information that could represent some form of exposure or breach or compromise of the infrastructure. One of the arguments against performing pen testing is that the nature of the tests that are run can destabilize different components of the infrastructure. In fact, ISO 27001 does not explicitly call for the execution of pen testing. The theory is that if an organization is doing all the other prerequisites with respect to security risk management, including effective vulnerability management program, network segmentation and the like, that you then have done all the necessary activities such that the actual execution of a pen test is rendered unnecessary. So you would not need to execute a pen test and subject yourself to the inherent risk that a pen test would represent.

MKM: Looking ahead to 2016, anything you see changing in terms of trends or demands from CEs to their BAs in terms of the sorts of assurance they are seeking or should seek?

DS: The healthcare industry is like some other industries, particularly financial services, where we are seeing much more heightened awareness of the risks that are represented by the BA. The interdependency of this elaborate web of business associates that supports our healthcare system is what makes it so great, and it's also increasingly, in conjunction with the very persistent and sophisticated cyber threat, what makes it so dangerous.

We are seeing increasingly where CEs are becoming more and more aware of these risks, and they are raising the bar on their BAs with respect to their expectations to demonstrate and to provide appropriate forms of evidence that they have done the right sorts of things, not just for HIPAA compliance but also for effective risk management. Because sometimes the nature of the cyber threat could be greater than what is called for by, for example, the HIPAA Security Rule.

So we are seeing an expectation to see evidence that you have thought through these risks, that you have really followed the spirit of what is called for by the risk analysis requirement from the Security Rule, and that you have taken a very thoughtful approach with respect to risk management.

That which is required by the HIPAA Security Rule is a good start, but it is not nearly enough for many organizations. And so we would suggest, if you are a BA and you represent any form of significant risk to your CEs, that you actually deploy protocols such as those represented by ISO 27001 or perhaps NIST 800-53; that you incorporate that into an effective risk management program; that you subject it to independent oversight, monitoring and testing; and that you be prepared, when it comes time for contracting with a CE, to be able to provide them with an independent form of assurance reporting to provide evidence for all of the above. SOC 2, when done properly, can provide that level of professional standards that we see more and more CEs calling for.

About Aprio

Since 1952, clients throughout the U.S. and across more than 40 countries have trusted Aprio for guidance on how to achieve what's next. As a premier, CPA-led professional services firm, Aprio delivers advisory, assurance, tax and private client services to build value, drive growth, manage risk and protect wealth. With proven expertise and genuine care, Aprio serves individuals and businesses, from promising startups to market leaders alike.

Aprio.com