HA+W | Aprio℠
The new name for HA+W

Passionate for what's next

Five Tenets of Effective Risk Management

WILL 'HIPAA COMPLIANCE' PROTECT YOUR HEALTHCARE ENTITY?

By Dan Schroeder, partner-in-charge of Information Assurance, Aprio

Healthcare is under attack. The information and infrastructure on which the healthcare sector relies is squarely in the sights of bad actors whose motivations range from ideological to nationalistic to crass monetization. This targeting is motivated largely by the value of healthcare records on the black market, which ranges anywhere from $40 to over $100 per record. The value of these records is derived from the rich personal information they contain, which can be used to build false identities, file false medical claims, score drugs, launch targeted phishing attacks and perform a plethora of other nefarious activities.

Today's sophisticated cyber threats—which include organized criminal and nation-state attackers—were unimaginable when HIPAA was devised. As a result, the risk management protections deployed by HIPAA covered entities (CEs) and their business associates (BAs) lag far behind the capabilities of their attackers.

Driven by rising healthcare costs, healthcare IT innovators are finding ways to vastly improve the quality and efficiency of healthcare processes while bringing costs down. Unfortunately, innovation is outpacing security, and most healthcare providers have been caught unprepared for this cyber-crime threat.

> "PHI is a uniquely challenging data set to protect. On the one hand, it is extremely rich in deep demographics and other highly sensitive information that should not fall into the wrong hands. At the same time, PHI needs to be available virtually on demand and is readily shared among providers, patients, payers and business associates."
>
> Redspin, Breach Report 2015: Protected Health Information

> "The pace of EHR adoption has consistently outstripped the ability of health organizations to adequately safeguard protected health information from significant breaches."
>
> Redspin, Breach Report 2015: Protected Health Information

In this article, we explain why HIPAA compliance will not protect your healthcare organization from disclosure or misuse of ePHI—and it won't even protect it from fines if that data is breached. Rather than a "check-the-box" compliance approach to vendor risk management, we will outline a more prudent and efficient risk management approach that will provide the greatest level of protection to your organization and all the individuals who entrust their data to it.

2015: The Year of the Healthcare Breach

2015 WAS HAILED AS THE "YEAR OF THE HEALTHCARE BREACH" FOR GOOD REASON:

The Department of Health and Human Services tracked 270 large data breaches that affected more than 113 million individuals that year.

That astounding number of breached records—the largest of any year by at least a factor of seven—accounted for about 67 percent of all large breaches of personal health information since HHS launched its "Wall of Shame" in 2009.

The top three breaches of 2015 (Anthem, Premera Blue Cross and Excellus Health Plan) affected a total of nearly 100 million records. These were also the largest PHI breaches of all time.

2016 is on track to close with more than 250 large breaches that exposed almost 15 million medical records—more than any other year except 2015. And nearly one-quarter of those records were exposed by incidents that involved a business associate.

What's going on here? Wasn't HIPAA conceived and implemented 20 years ago to safeguard this sensitive information while encouraging healthcare providers to use it to improve the quality of care?

What's Up with HIPAA?

Speaking of HIPAA, let's take a look at enforcement activity from the Office for Civil Rights (OCR). After pilot audits in 2011 and 2012, OCR indicated that it would resume its audits in 2014 and that this time they would include both covered entities and business associates.

In July 2016, OCR finally initiated desk audits of 167 covered entities—a full two years after first announcing them. Desk audits involving business associates were rumored to be kicking off in September—no, make that October, er… actually, November.[1]

One has to wonder whether HIPAA compliance is a particularly high priority for the OCR. Granted, its August 2016 settlement with Advocate Health System for $5.55 million represents the largest HIPAA-related financial penalty so far. Yet these fines are few and far between—leading some to describe HIPAA as a "toothless tiger." [2]

That said, the HIPAA tiger has the potential to grow very sharp teeth, and it currently has its eyes trained on business associates as the potential point of vulnerability.

Check-the-Box Compliance Will Not Protect You

Here's the rub: A superficial, compliance-oriented approach to vendor management will not protect your healthcare organization from disclosure or misuse of ePHI—or even from HIPAA related fines.

For one thing, when HIPAA was devised, the threats that exist today were nearly unimaginable. The freelance hackers of the 1980s and 1990s bear little resemblance to the sophisticated and highly organized nation-state attackers behind the Anthem, Premera and Office of Personnel Management breaches.

Here's another reason why HIPAA compliance is an insufficient approach to vendor risk management. Compliance has almost nothing to do with thoughtful analysis and management of risk, and it has almost everything to do with checking boxes.

1 GovInfoSecurity. "HIPAA Audit Update: Here's What's Next."

2 The Washington Post. "Your health records are supposed to be private. They aren't."

Whether those boxes relate to regulatory or vendor management approval, many healthcare executives are tempted to believe that a report from a credentialed third party means that their BAs are not only "compliant," but also that they have done all the right things to protect their valuable data and information systems.

Are the Right Things Happening?

Healthcare information security professionals know better. Rather than going along with this "check-the-box" mentality, CISOs and other security-minded leaders can become champions in their organizations by making sure the right things are happening with regard to protection of PHI.

By definition, compliance meets a minimum baseline that has been established by regulation or by customer contract. "HIPAA compliance" is a particularly troublesome concept. The vaguely-worded requirements leave much room for interpretation and provide little guidance to organizations about how to accomplish them. As a result, a number of "check-the-box" questionnaires (including HHS' own Security Risk Assessment Tool) have sprung up that purport to walk the user through the compliance process.

The inconvenient truth is that compliance reports cannot serve as a proxy for a company's ongoing, enterprise-wide risk management. And while one of the "boxes" that CEs and their BAs must check is an analysis of threats to confidentiality, integrity and availability of ePHI, very few organizations truly understand how to execute an effective risk analysis.

Putting in place a series of controls that match up with items on a checklist is not enough to protect the business from potential breaches—or, in the event of an actual breach, from substantial fines if plaintiffs' lawyers uncover vulnerabilities that they believe could have prevented the breach.

Today's cyber threats can only be effectively mitigated by conducting a thorough and accurate assessment of potential risks, followed by implementation of security measures to reduce those identified risks to a reasonable and appropriate level—in other words, the very things required by the HIPAA Security Rule risk analysis and risk management provisions.[3]

Five Tenets of Effective Risk Management

To protect their organizations and their patients, CEs need to demand evidence from their BAs of a sustainable information risk management program. This program must begin with a thoughtful assessment of risks that builds on a meaningful baseline security protocol, which in turn informs risk treatment options that are commensurate with the level of threat and the value of digital assets at risk.

The five tenets of this effective risk management approach include:

1. Set a baseline.
2. Assess risks to digital assets.
3. Apply risk management commensurate with risks.
4. Perform ongoing monitoring of controls.
5. Choose the right assurance reporting option.

> CISOs can become champions by making sure the right things are happening with regard to protection of PHI.

3 HIPAA §164.308(a)(1)(ii)(A): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the covered entity or business associate.
HIPAA §164.308(a)(1)(ii)(B): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a):

1. Ensure the confidentiality, integrity and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required.
4. Ensure compliance with this subpart by its workforce.

Set a baseline.

The first tenet of effective risk management is to assess the BA's existing controls against the requirements for a baseline security protocol and remediate gaps. In healthcare, that baseline primarily consists of the provisions of the HIPAA Privacy and Security Rules.

The implementation guidance found within the International Standards Organization's (ISO) 27001:2013 information security management framework provides detailed, practical language that clarifies and expands upon the high-level HIPAA Security Rule requirements.

Assess risks to digital assets.

The next tenet of effective risk management is to gain a realistic perspective on threats and resultant risks to confidentiality (i.e., security and privacy), integrity and availability (CIA) of protected health information.

For a healthcare IT company that provides EHR services, the combination of the EHR and the ePHI that it generates is considered a high-value digital asset that represents significant risks. The potential exposure of that ePHI could lead to damage to the brand, shareholder lawsuits and regulatory liabilities, among other risks.

By defining the value of digital assets at risk, the organization can focus its risk assessment efforts on those assets that represent the greatest value—as well as the greatest potential liability. As a result, information security professionals and business leaders have better information with which to allocate their information security money and resources.

Apply risk management commensurate with risks.

By adopting a baseline security program and expanding that baseline with enhanced controls based on the asset-based risk assessment, the organization creates a "superset" of criteria that addresses the full range of risks. This superset can be used as a basis for the design of controls that are in harmony with one another, as opposed to potentially repetitive or conflicting controls that can arise from a more disjointed approach.

Certain digital assets will represent higher risks that are not mitigated to an acceptable level by a baseline set of controls and will require enhanced mitigation efforts—or other risk management measures, such as risk transference through cyber insurance.

Perform ongoing monitoring of controls.

A centralized repository of control evidence makes monitoring of controls more efficient, and thus allows more frequent monitoring. Organizations that monitor and test controls throughout the year find that the process is more efficient and provides greater peace of mind. Ongoing monitoring and testing allows them to prioritize areas that were deemed most risky by the organization's risk assessment and gives them plenty of time to remediate those issues before any audits.

Choose the right assurance reporting option.

Many CEs and their BAs find that SOC 2, an internal control assurance reporting framework from the American Institute of Certified Public Accountants (AICPA), effectively fulfills their risk management and vendor management needs and provides the transparency their stakeholders expect.

The AICPA's service organization control (SOC) reports are performed under the institute's attestation standards. An attestation is a particularly

rigorous type of assurance engagement in which an independent CPA expresses an opinion on one or more assertions from management. Not only must CPAs comply with the AICPA's strict attestation standards, but they also bear professional liability for their opinions. So when independent CPAs attest to the suitability and operating effectiveness of an information system and its controls, they have personal and professional skin in the game. No other type of report provides this level of assurance.

SOC 2 is a scalable framework that can be expanded to incorporate subject matter in addition to management's description of the organization's system, as well as suitable criteria that are incremental to the AICPA trust services criteria. For example, as discussed above, many BAs find that the detailed criteria of ISO 27001 enhance their information risk management program.

Requirements set forth by HIPAA also can be incorporated into the SOC 2 reporting framework, as can the criteria of the HITRUST Common Security Framework, which was developed by the Health Information Trust Alliance (HITRUST) in collaboration with healthcare, technology and information security leaders.

Many CEs have incorporated the HITRUST CSF into their vendor management programs, and some require BAs to achieve HITRUST certification.

Our view is that a well-defined SOC 2 attestation that is based upon a thoughtful risk assessment meets both the letter and the spirit of the HIPAA requirements for risk analysis and risk management. **This is the case as long as the SOC 2:**

- Is performed by an independent CPA with the proper experience and professional judgment;
- Is based upon a sound risk assessment; and
- Encompasses criteria associated with those identified risks in the domains of security, privacy, availability and integrity.

This solid, risk-based groundwork enables the SOC 2 auditor to readily accommodate any incremental criteria that are relevant—whether those incremental criteria come from a regulatory standard such as HIPAA or an industry consortium such as HITRUST.

By focusing on suitable controls, rather than compliance with individual regulations and customer contracts, reporting becomes a byproduct rather than the focus of the process, and organizations build a robust information security management system that not only meets regulatory requirements, but also addresses the stakeholders' governance needs.

Beyond Compliance: Real Risk Management and Assurance

Regulators, clients, patients and plaintiffs' lawyers all are scrutinizing your healthcare organization's management of privacy and security risks to ePHI. A checklist approach to compliance will not provide the assurance that these stakeholders expect and the defense that your organization needs in the event of an actual security breach.

Healthcare organizations—like every other type of entity—struggle with lack of resources and bandwidth to dedicate to cyber security and vendor management. Not only does the risk management approach described in this paper represent the most effective approach, but it also is the most prudent path that enables CEs and their BAs to comply with HIPAA and vendor risk management requirements—and more importantly, it provides the best form of protection against threats to the valuable ePHI with which they are entrusted.

HA+W | Aprio
The new name for HA+W

Passionate for what's next

Five Concourse Parkway,
Suite 1000
Atlanta, GA 30328
404.892.9651
Aprio.com

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

Morison KSi
Independent member

Questions? Contact:

Dan Schroeder
Partner-in-Charge,
Information Assurance Services
dan.schroeder@aprio.com
770.353.8379