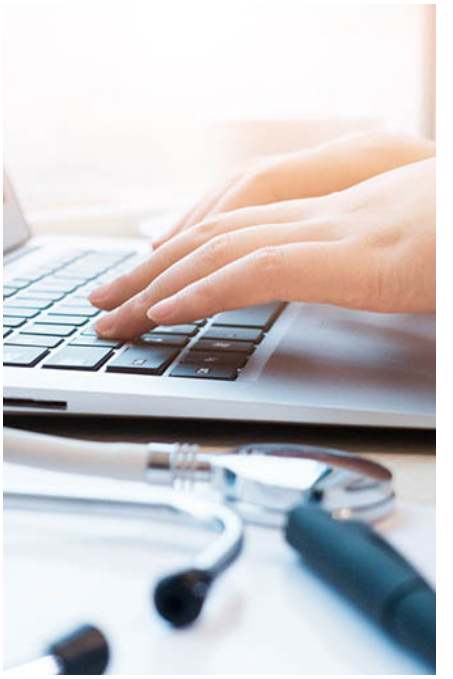
Aprio

Passionate for what's next℠

Beyond HIPAA 'Check-the-Box' Compliance

HOW HEALTHCARE IT COMPANIES CAN RAISE THE BAR ON DATA SECURITY

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



Breaches of protected health information (PHI) increased nearly 900 percent in 2015, according to Department of Health and Human Services (HHS) data.

Granted, 2015 was an anomaly. The vast majority of those breached records are attributed to three large health insurers (Anthem, Premera Blue Cross and Excellus). But 2016 is on track to close with more than 250 large breaches (those affecting 500 records or more) that exposed almost 15 million medical records—more than any other year except 2015.

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?

And yet, more than 1,700 large breaches have been reported to HHS since the department started requiring breach notifications seven years ago.

More than 1,700 large breaches have been reported to HHS since the department started requiring breach notifications seven years ago.

Compliance Does Not Equal Risk Management

There are a couple of reasons why HIPAA compliance is an insufficient approach to risk management. For one thing, when HIPAA was devised, the threats that exist today were nearly unimaginable. The freelance hackers of the 1980s and 1990s can't even be spoken of in the same breath as 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 won't deliver 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.

Whether those boxes relate to regulatory or vendor management approval, many healthcare IT leaders are tempted to believe that a report from a credentialed third party means that they are not only "compliant," but also that they have done all the right things to protect their valuable data and information systems. HIT leaders should resist this tendency and instead embrace their responsibility for 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 covered entities (CEs) and business associates (BAs) must check is an analysis of

For a business that is built on its ability to compile and manipulate large volumes of ePHI, a cyber breach could put the entire value of the business at risk.

threats to confidentiality, integrity and availability of ePHI, very few organizations truly understand how to execute an effective risk analysis.

And yet, 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 risks to a reasonable and appropriate level—in other words, the very things required by HIPAA.

Value at Risk

Another driver of today's unprecedented level of healthcare breaches is the impressive value of healthcare records on the black market—anywhere from $40 to $100 per record or more.

The value those records represent to the organizations that leverage them for competitive advantage is much greater. For a business that is built on its ability to compile and manipulate large volumes of ePHI, a cyber breach could put the entire value of the business at risk.

For starters, if healthcare providers doubt the privacy and security of their patients' ePHI, healthcare IT companies are dead in the water. And companies planning an IPO or equity investment could see the deal fall apart if a significant security vulnerability was discovered during due diligence.

Raise the Bar Beyond HIPAA Compliance

The value of your business depends on a logical and reasoned approach to managing the privacy and security of ePHI—not a check-the-box approach that merely achieves (or purports to achieve) compliance.

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.

Healthcare IT companies need to demonstrate that the business has put in place a sustainable information risk management program that first and foremost protects ePHI and also complies with client contracts and HIPAA privacy and security rules. This program must begin with a thoughtful assessment of risks that leads to meaningful design of controls. The final piece of the puzzle consists of rigorous independent testing and reporting that provides a high degree of transparency into the information risk management process.

1. Understand risks to your most valuable assets.

All data are not created equal. Certain data sets are used in mission-critical business processes to drive significant value. These combinations of data and business processes are known as digital assets.

For a healthcare IT company that provides electronic health record (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 focusing on the value of digital assets at risk, the organization can conduct a more focused risk assessment that uncovers the most significant risks to the organization. As a result, information security professionals and business leaders have better information with which to allocate their information security money and resources.

2. Raise the bar on cybersecurity through a sustainable information risk management program.

An asset-based risk assessment tells the organization where it needs to raise the security bar—but not how. Within the context established by that risk assessment, the organization must establish its own set of criteria for how it must manage those risks.

For example, healthcare providers use their EHR systems during patient encounters as well as business operations, and so they expect the highest level of confidentiality of ePHI, as well as high availability and integrity of the systems. Within these domains (confidentiality, integrity, availability), the company can write specific criteria that will form the backbone for its design of controls and for auditors' tests of those controls.

When forming these criteria, a robust internal controls framework such as the International Standards Organization's (ISO) 27001:2013 standard can provide a solid baseline.

The implementation guidance found within the ISO 27001 standards provides detailed, practical language that clarifies and expands upon the high-level HIPAA Security Rule (HSR) requirements. For example, whereas the HSR requires CEs and BAs to "assign a unique name and/or number for identifying and tracking user identity," ISO provides detailed guidance on the process for managing user IDs, authenticating those IDs and assigning or revoking access rights.

Encryption is another area where ISO dives far deeper than the HIPAA requirements. Whereas HIPAA says, "implement a mechanism to encrypt and decrypt electronic protected health information," ISO provides implementation guidance on what to include in a cryptographic policy, as well as how to identify and classify the information that should be encrypted.

ISO 27001 is not another "check-the-box" list of internal controls; it is a comprehensive framework for an information security management system that elevates cybersecurity from a series of technical controls owned by the IT department to an enterprise-wide culture of security characterized by continuous improvement.

3. Put your best foot forward with the right assurance reporting.

Management, boards, customers, prospects and regulators increasingly require assurance reporting that tells them:

- Which information assets are at risk
- How you are assessing risks to that information
- How you are managing those risks
- How you are testing those controls

But which assurance reporting is right for a BA? 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.

ISO 27001 is not another "check-the-box" list of internal controls; it is a comprehensive framework for an enterprise-wide, sustainable information security management system.

WHICH INFORMATION ASSETS ARE AT RISK?

HOW ARE YOU ASSESSING RISKS TO THAT INFORMATION?

HOW ARE YOU MANAGING THOSE RISKS?

HOW ARE YOU TESTING THOSE CONTROLS?

Aprio

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

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 additional 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 can strengthen 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 assessment 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 to the BA's ePHI—whether those incremental criteria come from a regulatory standard such as HIPAA or an industry consortium such as HITRUST.

Your Cybersecurity Voice of Reason

Regulators, clients, patients and plaintiffs' lawyers all are scrutinizing your 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 business needs in the event of an actual security breach.

The only defensible approach is one that begins with a thorough assessment of the actual risks to your most valuable assets and builds on a meaningful information security framework. This approach is the most prudent path for BAs seeking to comply with requirements of regulators and CEs—and more importantly, it provides the best form of protection against threats to the valuable ePHI with which they are entrusted.

Morison KSi
Independent member

Questions? Contact:

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