Aprio

Passionate for what's next®

Beyond 'Check-the-Box' HIPAA Compliance

HOW HEALTHCARE IT COMPANIES CAN RAISE THE BAR FOR DATA SECURITY

By Dan Schroeder, Partner-in-Charge, Information Assurance

Patient records are "cyber gold." Healthcare organizations of all sizes and their third-party business associates and service providers need to face the fact - they are primary targets for cyber criminals. Today's mechanized industrial hacking operations don't care how big you are. They are constantly scanning and finding security vulnerabilities.

The government agency that enforces HIPAA privacy, security and breach notification rules, the Office for Civil Rights (OCR), posts all reported healthcare breaches affecting over 500 individuals on a public web page. This URL is infamously referred to as the "Wall of Shame." At the end of Q3 2020 there were nearly 330 cases under investigation, affecting over 12.6 million individuals identified on the Wall of Shame - a 30% increase over 2019.

Compliance does not equal risk management

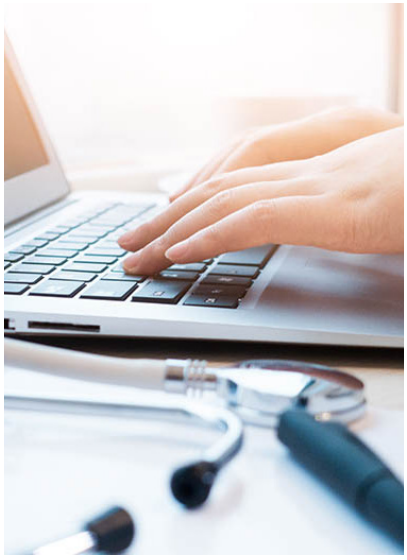
There are two reasons why HIPAA compliance is an insufficient approach to risk management. First, when HIPAA was devised, the threats that exist today were unimaginable. The freelance hackers of the 1990s are incomparable to the sophisticated and highly organized nation-state attackers behind today's breaches.

The second reason HIPAA compliance won't deliver risk management is that compliance has little to do with the thoughtful analysis and management of risk. Compliance is about 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 everything necessary to protect their valuable data and information systems. But that simply isn't true. Healthcare IT leaders need to embrace their responsibility for making sure the right things are happening to safeguard 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. HIPAA's vaguely-worded requirements leave much room for interpretation and provide little guidance to organizations on 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 the user to walk 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. One of the "boxes" that Covered Entities (CEs) and Business Associates (BAs) must check relates to an analysis of risks to confidentiality, integrity and availability of ePHI. Unfortunately, very few organizations truly understand how to execute an effective risk analysis.



HIPAA has been in place since 1996, yet the number of privacy and security cyber incidents continue to rise. Clearly "compliance" is not enough.

Aprio

Passionate for what's next®

Understanding the value at risk

If healthcare payers and providers doubt the privacy and security of their ePHI in the hands of a BA or healthcare IT service provider, that company is dead in the water. Healthcare IT companies need to consider the following factors to fully understand the value at risk and the importance of information risk management to the business.

- The value to cyber criminals – The key driver of the unprecedented rise in healthcare breaches is the impressive value of healthcare records on the black market–up to $1000 per record. This is due to the wealth of PII and ePHI contained in these records.
- Protection of the business model and its value – For a business that is built on its ability to compile and manipulate large volumes of ePHI, a cyber breach places the business model and entire value of the business at risk.
- Investor IT due diligence – Companies that are planning for IPO or equity investment should realize that a deal can easily fall apart if a significant security vulnerability is discovered during due diligence, let alone an ongoing investigation of a reported breach.

Raising 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 they have implemented a sustainable information risk management program that first and foremost protects ePHI and also complies with client contracts and HIPAA privacy and security rules.

Effective risk management programs must begin with a thoughtful assessment of risks that leads to a 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 digital assets.

All data is 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. This provides a more informed approach to prioritizing corrective actions and the allocation of time, money and resources.

2. Playing the long game with assurance partners and 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

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

Which information assets are at risk?

How are you assessing risks to that information?

How are you mananging those risks?

How are you testing those controls?

Aprio

Passionate for what's next®

True Information risk management is an iterative process that requires continuous monitoring and testing. Effectively managing cost and achieving constant improvement require long-term planning and thoughtful execution. Therefore, it's critically important to select a vendor that will work with you as a long-term partner to advance the privacy and security objectives of the business as it grows and matures.

A full-service CPA advisory firm that has strong technology industry expertise and an experienced information assurance and risk management practice represents a good option over specialized compliance reporting providers for two reasons.

First, a specialized compliance reporting provider may be more interested in generating reports than actually assessing risk management practices. A full-service CPA advisory firm will take a more wholistic view of the business, partnering with businesses to advance operational integrity and profitability over time.

Second, many CEs and BAs prefer efficacy of CPA attestation reports. 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.

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.

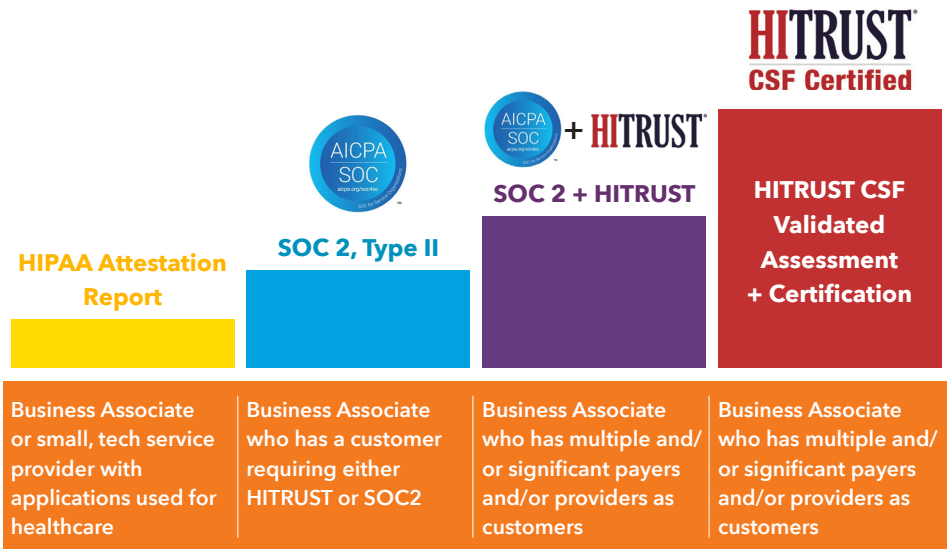
> Effective risk management must begin with a thoughtful assessment of risks that leads to a meaningful design of controls and rigorous independent testing and reporting.

Choosing the right level of risk management and compliance

The ability to demonstrate compliance with HIPAA and the growing list of privacy and security standards is key to business growth. But how do you select the right level of risk management and compliance reporting for your business and role as a BA?

Information risk management and HIPAA compliance is not a one size fits all proposition. Options can include HIPAA Attestation Reports, SOC 2 Type II, SOC 2 + HITRUST and HITRUST CSF Certification. Determining the right option requires consideration of relative cost, the maturity of the business and the requirements of customers and prospects.

HIPAA compliance reporting options by cost, complexity and customer requirements.



Aprio

Passionate for what's next®

HIPAA Attestation Reporting – the easiest and most cost-effective assurance reporting to achieve. It is appropriate for startups and generic technology service providers that offer applications that can be used in healthcare and have minimal interaction with ePHI. The business may have 1-2 customers requesting HIPAA compliance and/or HITRUST CSF or SOC 2 reporting.

SOC 2, Type II – the next step up, SOC 2, Type II, applies when the company is classified as a true Business Associate and therefore needs to meet the "spirit and intention of HIPAA." Given the potential synergies between SOC 2 and HITRUST CSF, SOC 2, Type II is often a good option for BAs that have a customer that will accept either a HITRUST CSF Validated Assessment or a SOC 2, Type II report.

SOC 2 + HITRUST – should be considered by BAs that have multiple and significant payers and/or providers as customers. This reporting structure is applicable when a customer requests SOC 2 Type II reporting and evidence that the BA meets HITRUST requirements. SOC 2 + HITRUST is considerably easier and more cost-effective to achieve than HITRUST Validated Assessment and Certification.

Becoming HITRUST CSF Certified – The HITRUST CSF has become a widely adopted security and privacy framework across industries globally. However, the cost and complexity of HITRUST CSF Validated Assessment and Certification should only be undertaken when specifically requested by a customer. BAs that serve multiple and significant payers and/or providers such as hospitals and insurance companies may be required to be HITRUST CSF Certified.

Your Compliance Voice of Reason

As the connectivity between payers, providers and patients continues to advance, healthcare IT companies face increasing business opportunities and risks. Regulators, clients, patients, investors and legal teams are all positioned to scrutinize your organization's management of privacy and security risks to ePHI. A checklist approach to compliance will not provide the assurance these audiences expect and the defense your business needs in the event of a security breach.

To keep your business off the Wall of Shame, the only defensible approach is one that begins with a thorough assessment of the actual risks to your most valuable assets and builds on meaningful information security frameworks and the long-term objectives of the business. 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.

Aprio is the only top 50 CPA Firm with a specialization in healthcare IT. As a premier provider of the assessment and attestation services healthcare IT companies need, Aprio has deep experience in HIPAA Attestation Reporting SOC2, ISO 27001, ISO 27701 and HITRUST CSF Validated Assessment and Certification.

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

Morison KSi
Independent member

Got HIPAA Compliance Questions? Contact:

Dan Schroeder
Partner-in-Charge, Information Assurance Services
dan.schroeder@aprio.com
770-353-8379