HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

February 2017

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

Promoting a culture of compliance in daily operations and business goals

an interview with Darrell Contreras
Chief Compliance Officer
Millennium Health
San Diego, CA

See page 18

by Dawn Lambert and Chris Luoma

Healthcare's new reality: Preparing for and managing an OCR business audit

» HIPAA plays a critical role in ensuring the confidentiality and privacy of protected health information.
» The OCR conducts comprehensive audits annually to ensure ongoing compliance.
» Business associates can now be held accountable for data breaches.
» Centralize and organize business associate agreements and compliance-related information.
» Audit preparedness begins at the top. Designate a leader or team to monitor all compliance activities and processes.

Dawn Lambert *(delambert@iasishealthcare.com) is Chief Privacy Officer at IASIS Healthcare in in Franklin, TN and* ***Chris Luoma*** *(cluoma@ghx.com) is Vice President Product at GHX in Atlanta, GA.*

Many advances in medicine have been made over the past 20 years, transformative changes that have increased the safety and efficacy of healthcare. One of those changes was the passage of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). It continues to send ripples throughout healthcare and plays a critical role in the confidentiality and privacy of protected health information (PHI). Violating that privacy or mishandling the information is the compliance equivalent to medical malpractice.

How we got from there to here

HIPAA has progressively evolved from a means to modernize information exchange in healthcare to include Privacy, Breach Notification, and Security Rules as well as compliance audits. In 2011, the Health and Human Services Office for Civil Rights (OCR) began a pilot program during which 115 covered entities were audited to gauge the level of HIPAA compliance.[1] The audits were onsite, comprehensive reviews of compliance activities. It is believed that only 11% of covered entities passed.[2]


Lambert


Luoma

In 2013, the final Omnibus Rule was issued and the industry was given six months to comply. One of the important components of the Rule was that business associates (BAs)—a person or entity that creates, receives, maintains or transmits protected health information (PHI) on behalf of, or provides services to, a covered entity—could now be held liable for data breaches. The inclusion of BAs put thousands of companies on notice that PHI and ePHI was the responsibility of all in the industry.

BAs have come under the magnifying glass of the OCR for good reason. Although 58% of breaches came from covered entities, 62% of the records came from BAs.[3] The government now understands that BAs are

maintaining, in some manner, a large volume of this PHI.

OCR, the organization responsible for enforcing the HIPAA Privacy and Security Rules, began Phase 2 audits in July 2016. The program was redesigned based on insight from the initial pilot audits as well as updates to the law. Notifications were sent to 167 covered entities that were chosen to participate in the desk audits, requesting documentation of specific policies, procedures, and evidence of compliance. Step One in the new day of OCR audits had begun.

What followed were requests for information to enable the OCR to review the policies and procedures of both covered entities and requests for covered entities to identify their business associates. Phase 2 audits comprised 200 – 250 audits in total; the majority were desk audits.

The information organizations are required to provide:

- Business associate name
- Type of services provided
- Two points of contact, including name, address, phone, fax, and email
- The website URL, if applicable

Underscoring all of this is the responsibility of the covered entity to assess the risk the BA poses before entrusting them with PHI. The financial ramifications from a misstep are significant. The average cost of a breach is $3.8 million. At the high end, the cost is $1,000 per record stolen with the average cost per record roughly $350.[4] Protected health information is serious business.

The new reality in healthcare is that the audit is a business requirement to not only know about, but also understand and be thoroughly prepared for. The audits are here to stay, but the protocols will likely continue to change as technology and the needs of healthcare privacy and security change.

Start with a leader

One of the strongest best practices when it comes to compliance and managing the new audit requirements is having a leader, ideally in the Privacy Office, who has strong relationships across the organization. Identifying and gathering the necessary BA information touches every part of an organization, and relationships across functions will be vital to success. BA information lives in information technology systems, clinical settings, the Legal and Finance departments, and more.

Collaboration is key. To put the best preparation measures in place, it will take a dedicated team to be the eyes and ears of the organization. Having people across the organization who understand the value they bring to compliance and the role they play in protecting not just the organization, but actual patient information, must become the cultural norm.

And, it's not just the Compliance department that should be concerned about protecting the organization. The C-suite must engage fully in the organization's compliance activities, because the risk to the organization spans all departments. Understanding the responsibilities and concerns of each department can help make the compliance process more complete. Table 1 (on page 36) shows some of the most important concerns.

The compliance management process

Out of the thousands of covered entities in the United States, only a very small percentage received notification of a Phase 2 audit. But for those selected, they had just 10 business days to respond after the notification was received. Bottom line, if the documentation and risk assessments haven't already been collected or conducted by the time the notification arrives, it's most likely too late. The volume of information required is large, and it must be validated and sent digitally.

Table 1: Typical concerns of healthcare departments.

Type of Risk	Purview of	Issues
Regulatory	Chief Compliance Officer	Regulatory risk; being on the "radar screen" for one issue often makes you visible for others
Security	Chief Privacy Officer	Similar to CIO – HIPAA Privacy and Security
Financial	Chief Financial Officer	Threats to profitability, bond rating, insurance premiums
Technology	Chief Information Officer	Many failures are related to technology safeguards
Reputational	Chief Marketing Officer	PR crisis and loss of "trusted community provider" status
Patient Safety	Chief Nursing Officer	Patient safety compromised; adverse outcomes
Operational	Chief Operating Officer	Threats to business continuity, operational efficiency, risk of revocation of necessary permits, licenses, etc.
All	CEO	All of those listed above, but especially profitability and reputation

That doesn't mean the remaining covered entities are off the hook. The OCR audits will be conducted annually. Covered entities should expect to face an audit in the future, and the best course of action is to prepare today.

The place to begin preparation is reviewing the OCR audit protocols and the compliance management process itself. The audit not only identifies vulnerabilities, but also it presents an opportunity for covered entities to improve this process, including the use of automation. Most organizations discover that they are managing their BAs with a spreadsheet and a file cabinet. It may be fine as a starting point, but the requirements of an audit will quickly swamp a Compliance department's ability to manage the information. Plus, there are too many BAs to manage the information manually.

The use of readily available tools, including vendor management and compliance document management systems, reduces the complexity and improves the accuracy and the comprehensive collection of necessary data. A central repository is crucial to audit readiness.

Under the HIPAA rule, healthcare organizations must identify which of their vendors are classified as BAs, and have a signed and executed business associate agreement (BAA) for each of these vendors. For those BAs that have failed to sign BAAs, healthcare organizations need the ability to show the steps they have taken to try to secure agreements.

Centralizing and streamlining the BA management process gives an organization the ability to quickly and efficiently reach out to all BAs to obtain these agreements, confirm that vendors have current risk assessments and procedures, and manage the ongoing education necessary to stay current. Vendor management technology makes this so much easier and more consistent for visibility and control. In fact, in today's healthcare and business environment, it's the only way.

The process of collecting all this data can yield some unwelcome surprises. The organization may underestimate the challenge, thinking it has only a hundred BAs when in fact it has thousands. Plus, the process by which vendors interact with the organization is more like a maze than a highway. These revelations and challenges should be viewed

as an opportunity, giving a covered entity an opportunity to identify potential gaps and the ability to rectify them before an audit.

Capturing the information is only one aspect of being prepared. The audit process has shown that keeping the information current is perhaps as large an undertaking as collecting the data in the first place. An ideal practice is to reassess BAs from a risk and compliance standpoint every six months. Once started, it's a process that will repeat.

There are five basic steps in the process of risk assessment and compliance. The following are the questions that can identify the actions needed to both secure and protect PHI and ePHI. These steps can also guide the preparation for any audit requests for information:

- **Use contracting data:** With whom are you doing business? What will they do for your organization?
- **Use credentialing data:** What risk does the company pose to the organization? Once you've identified a potential BA, assess its risk profile. Has it had breaches in the past? Has the company taken the necessary corrective action?
- **Initiate and maintain communication and proof of compliance:** How is the company protecting your organization's data? Does it have all the necessary security requirements in place?
- **Follow up on processes:** Is the company continuing to improve processes? Are you educating the company on best practices and new procedures?
- **Ongoing management:** How are you monitoring and reporting on their compliance?

Conducting a risk assessment is required for both covered entities and BAs to identify risk. Risk assessments should be performed at least annually, more often if there's a change in environment. It's not just a "once and done" activity. As a covered entity, knowing the maturity of the partners you are doing business with is another part of helping to ensure that PHI and ePHI remain secure. That assessment guides all of the next steps.

At the HIMSS16 conference, a helpful model was presented that can guide this vendor assessment.[5] The five levels of maturity are from lowest to highest:

Aware: Development of high-level scope and program;
Reactive: Assessment on new relationships;
Adaptive: Assessments tailored to risk tier, managed remediation process;
Purposeful: Assessment depth/breadth appropriate for due diligence required, validation and tracking of remediation; and
Strategic: Scope focused on full spectrum of BAs, strong partnerships established.

The goal is to continuously move BAs in the lower levels of maturity into the more purposeful and strategic levels. Education and ongoing communication are central to helping move organizations to great maturity in their understanding and practices for protecting confidential data.

A final word

Preparing an organization for audits and increased compliance is the new reality of healthcare. It's no longer a good thing to do; it's an imperative. Be methodical and have a plan. Review the audit protocol thoroughly and research the excellent resources available online. After reviewing the protocol, conduct a risk analysis. This is the most common area of failure, and it should be afforded significant attention. The Office of the Inspector General publishes an annual Work Plan. A close review of the most current OIG Work

Plan for potential security and privacy audit projects is advisable. And finally, implement a compliance document manager solution to manage BAs and the documentation of audit processes. The accuracy, visibility, and control will help ensure that any requests for information can be easily addressed.

The biggest challenge to improving compliance is educating frontline employees without overwhelming them. They may not need to know how to build a firewall, but they do need to understand how to protect PHI and why that is so important. One of the easy holes to plug is educating employees on basic phishing and spoofing attacks. Employees can become one of the biggest assets in protecting the organization, rather than a significant liability due to lack of education.

Another significant challenge is controlling and tracking the exchange of data with and about vendors. Technology and specific vendor management and compliance document management solutions can improve compliance, but converting from a manual system can prove to be a challenging process.

Centralizing and organizing BAAs and compliance-related information increases accuracy and control. Simply knowing and tracking with whom PHI is being shared is a huge step in the right direction. And, having the ability to quickly and efficiently communicate to all BAs streamlines the management process.

No system is perfect, but creating effective processes combined with technology mitigates risk. And that is most certainly the goal.

1. Department of Health and Human Services: HIPAA Privacy, Security & Breach Notification Compliance Audits, Phase 2 Informational Webinar. July 13, 2016. Available at http://bit.ly/2iN5i0n
2. Smart Training blog: "HIPAA@20: Timeline" April 22, 2016. Available at http://bit.ly/2i7X2Y5
3. Ponemon Institute: 2015 Cost of Data Breach Study: Global Analysis. May 2015. Available at http://bit.ly/2i82OJq
4. Idem.
5. Health Information Management Conference and Exhibition, February 29 – March 4, 2016 in Las Vegas. More information at http://bit.ly/2hP9TCy