HIPAA Security Rule — Demystified

By Yigal Rechtman and Kenneth Rashbaum

In Brief

Fines under the Health Insurance Portability and Accountability Act (HIPAA) are formulaic, with little room for discretion, so a small medical office can suffer similar consequences as a large hospital if a breach has occurred. Thus, the degree of pre-breach preparation is pivotal. This article dispels the myths surrounding HIPAA compliance preparation so that advisors can prepare businesses for a possible data breach in a fairly painless, pragmatic manner. It will explore the significance of the interaction between the worlds of HIPAA compliance and practical policies and procedures (the purview of management and supported by an entity's legal advisors), which are often heavy with technical detail, and the risks associated with information systems and information technology (supported by internal IT professionals and third-party consultants). The good news is that, with HIPAA, an ounce of preservation can save a pound of *gold*, and a deliberate effort can be efficient, improve compliance, avoid penalties, and even contribute to greater business success.

When HIPAA was established in 1996, it was considered a paradigm shift in the U.S. healthcare industry. Although various federal and state regulations existed before HIPAA was enacted, the rules were dispersed among several statutes, and adherence and application of these laws was inconsistent at best.

Generally, HIPAA applies to several classes of entities. Two of those classes are "covered entities" and "business associates." Covered entities are hospitals, doctors, insurance companies, and healthcare clearing houses. Business associates are companies that transact during their normal course of business with covered entities. These applications are mentioned in several sections of the law. Two important sections are the Privacy Rule, which governs what is the appropriate treatment for patient information, and the Security Rule, which governs the safeguard of information from unauthorized access. Although the Privacy and Security rules apply to all manner of Protected Health Information (PHI), the Security Rule has a particular application when it comes to Electronic Protected Health Information (ePHI), safeguarding patient information in electronic form.

History of HIPAA Enforcement

For about a decade after the law was enacted, HIPAA enforcement was perceived as relaxed. Initially, there was a substantial effort—mostly by covered entities—to comply with the law. However, as years went by, regulators mostly relied on self-regulation and "best effort" approaches, and referral for action was a rare occurrence.

Action has been increasing in the past few years. Several high-profile security breaches to non-healthcare entities have made regulators reconsider their role in regulating the healthcare industry. For example, according to a 2013 report by the United States Department of Health and Human Services, complaints related to violations of the HIPAA rules increased 8% per year on average since 2003 (http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/complaintsyear.html). An average of 7,550 complaints per year were noted for 2004–2009; the average rose to 9,413 complaints per year for 2010–2012 (a 25% increase). The dollar amount associated with fines has also increased significantly, mostly due to the prescriptive nature of the law as it was amended in 2010. Regulators now have limited discretion in assessing fines; instead, fines are almost formulaic and based on length of the violation and other qualitative factors.

Consultants who have assisted entities and business associate have noted that a good-faith effort to understand and comply with the regulation goes a long way toward avoiding complaints and inquiries from regulators.

With the increased focus on greater enforcement and higher fines, consultants who are active in this field, business owners in the healthcare world and their advisors, and covered entities and their advisors must pay close attention to the HIPAA rules, which can be onerous to understand and observe.

Understanding the HIPAA Security Rule

The Security Rule's main objective is to protect ePHI and its operation and maintenance by the covered entity as well as, for all intents and purposes, the related business associate. It contains a list of required and addressable steps. The required steps have to be followed without regards to the entity's judgment, while the addressable steps can be disregarded if the reasons for doing so are documented.

For example, business associates and covered entities are *required* to maintain a disaster recovery plan. Simple responses such as "We have tape backup" or "We copy some files to a memory stick (from time to time)" are not sufficient. Rather, entities must have a documented disaster recovery plan that considers all aspects of its operations—including non-technology aspects—and the entity's response to the identified risks. In such a scenario, the presence of a tape backup is not relevant to a disaster that stems from a breach into the network and theft of ePHI.

By contrast, an addressable requirement, such as having an encryption mechanism for ePHI, is not a required step. The law only requires that entities *address* the risks of an ePHI breach, and having encryption is an optional method. (See http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf for further information.) However, if an entity (or a business associate) determines that the risk of such a breach is low, and that encryption of ePHI is not necessary, they need only document this evaluation, thereby addressing the requirement without taking any further action.

The requirements of the Security Rule can be readily understood and implemented. Consultants who have assisted entities and business associate have noted that a good-faith effort to understand and comply with the regulation goes a long way toward avoiding complaints and inquiries from regulators. For example, a business associate that was well aware of its HIPAA requirement acted swiftly when a list of patients was e-mailed to the wrong recipient. The business associate enacted its breach notification protocol, not only averting an embarrassing disclosure, but also appearing professional to all parties who were aware of the situation. Because the business associate was ready and trained, the affected parties awarded more business to that company, confident that it was in good standing with compliance.

On the other hand, lack of compliance can lead to a denial of coverage for professional malpractice insurance. In many policies,

compliance with laws and regulations is a standard clause. Medical providers that cannot document compliance with HIPAA may face a denial of coverage by insurance carriers.

HIPAA Compliance: Where to Begin?

Advisory professionals who wish to start complying with HIPAA should assemble an internal team comprising top management, IT professionals, and representatives of the production line. For example, if a CPA firm conducts audits of covered entities, the HIPAA team should include a representative of the executive committee, the IT group, and a representative from the audit group who knows what work is being performed in the field. If the covered entity is a medical practice, a similar team should be assembled consisting of management, a representative provider, and the IT professional with knowledge of the IT environment.

Because the Security Rule is a pervasive part of HIPAA, involvement of an IT professional cannot be replaced. However, not all steps are IT related, and at times outside legal counsel as well as other providers (e.g., an insurance agent) should be involved.

In following the compliance process, risk assessment is the first—and most important—step. The team should understand what HIPAA is, and in particular what PHI and ePHI are. Following that, the team should assess the risks to PHI and ePHI. These risks may be technological but also manual; one common practice risk is the misplacement or misfiling of patients' paper charts during the normal course of the day. This is a "manual" process that a medical practice will have to assess with respect to PHI.

After identifying technological and other risks, the internal team should attempt risk management as its second compliance step by addressing existing mitigation procedures. One potential case is a breach through the introduction of a malware, or a computer virus. Mitigation is often already present in the form of the pre-installed anti-virus software that nearly all businesses currently have in place. Nonetheless, it is important to first identify *all* the risks, and only then try to see what risk management solutions are already at hand. Sometimes the solution is not yet implemented, and the team may need to propose such solutions to upper management. This is especially true if the implementation requires significant effort and the allocation of resources.

The third step of the compliance process follows mostly from the first two (risk assessment and risk management). As stipulated by HIPAA, both the required and addressable steps must be completed and documented. It is important to note that HIPAA requires documentation of all thought processes, compliance with requirements, decisions made, and incidents reported. Recollection from memory is simply not an option. CPAs are in an excellent position to assist clients in performing such documentation.

HIPAA compliance is becoming an increasingly serious matter, and it is something that CPAs should be aware of.

Finally, the HIPAA regulation requires some degree of monitoring. Although an entity may theoretically conclude that monitoring is not a high priority (i.e., the risk is so low that there is no further need to comply), its management may decide to monitor, to some degree, the entity's compliance with HIPAA. This can be done in various ways and by various departments. In large entities, internal audit functions often are charged with such compliance. In smaller entities, an outside consultant may be the right driver and subject matter expert to perform and document the monitoring process.

A Word to Financial Auditors of Covered Entities and Business Associates

Compliance with laws and regulations is a consideration required by U.S. Generally Accepted Auditing Standards. (See AU-C section 250, "*Consideration of Laws and Regulation in an Audit of Financial Statements*," at http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-C-00250.pdf.)

AU-C section 250.05 requires that, among other things, "in conducting an audit of financial statements, the auditor takes into account the applicable legal and regulatory framework." Although further discussion of the compliance and its effect on audits follows from this statement, the financial effects and risks emanating from enforcement were often considered insignificant in previous years. Based on the Department of Health and Human Services statistics cited above, however, knowing that enforcement levels are increasing—and that the financial ramifications are growing—may change the auditor's consideration.

Accordingly, noncompliance of audit clients may be a state that the auditor should consider more closely for covered entities and even business associates. Noncomplying entities could face stiff fines and regulatory action (which is criminal) and their audited financial statements could be materially affected.

HIPAA compliance is becoming an increasingly serious matter, and it is something that CPAs, as well as other business advisors, should be aware of. Compliance with HIPAA is an interactive process that is achievable with some advice from professionals, training, and good-faith effort from both covered entities and business associates. In particular, early and active involvement of managers—alongside IT professionals and consultants—can enable compliance as well as support business success.

Yigal Rechtman, CPA, CFE, CITP, CISM, *is a director for information technology, technology assurance, and forensic services at Grassi & Co. CPAs LLP, Jericho, N.Y., as well as an adjunct professor at the Lubin School of Business, Pace University, New York City. He is a member of* The CPA Journal *Editorial Board.* ***Kenneth Rashbaum, JD,*** *is a partner at Barton LLP.*