HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY

Volume Twelve
Number Five
May 2010
Published Monthly

Meet

Miaja Cassidy Director of Healthcare Compliance at Target

PAGE 14

Earn CEU Credit

WWW.HCCA-INFO.ORG/QUIZ — SEE PAGE 41

Feature Focus:

Managing security risks in business associate relationships

PAGE 32

COMPLIANCE 101: INTEGRATING THE HOSPITAL COMPLIANCE PROGRAM WITH THE MEDICAL STAFF BYLAWS

PAGE 23

feature focus

Managing security risks in business associate relationships

By Michael R. Overly, Esq.; Chanley T. Howell, Esq.; and Lisa J. Acevedo, Esq.

Editor's note: Michael R. Overly is a Partner in the Los Angeles office of Foley & Lardner LLP and a member of the firm's Information Technology & Outsourcing Practice Group. His practice focuses on drafting and negotiating technology-related transactions. Michael may be contacted by e-mail at moverly@foley.com.

Chanley T. Howell is a Partner in the Jacksonville office of Foley & Lardner LLP and a member of the firm's Information Technology & Outsourcing Practice Group. His practice focuses on drafting and negotiating technology-related transactions, and counseling clients on records and data management issues. Chanley may be contacted by e-mail at chowell@foley.com.

Lisa J. Acevedo is a Partner in the Chicago office of Foley & Lardner LLP and a member of the firm's Health Care Industry Team and Privacy, Security and Information Management Industry Team. Her practice focuses on HIPAA and other federal and state privacy laws. Lisa may be contacted by e-mail at lacevedo@foley.com.

Newspapers and trade journals feature a growing number of stories detailing instances in which organizations have entrusted their most sensitive information and data to a vendor or other business partner, only to see that information compromised because the vendor failed to implement appropriate information security safeguards. Worse yet, those same organizations are frequently found to have performed little or no due diligence regarding their vendors and have failed to adequately address information security in their vendor contracts. In many instances, this leaves the organizations without a meaningful remedy for the substantial harm they have suffered as a result of a breach or compromise. That harm may take a variety of forms: damage to business reputation, loss of business, potential liability to the data subjects, and regulatory and compliance issues. Recent studies by the Ponemon Institute have shown that on average a company will pay $202 per record compromised and, in the aggregate, an average of $6.6 million if they experience a security breach.[1]

Those organizations, entities, and individuals that provide health care services possess extremely sensitive and valuable information about patients, including both health and financial information. In today's business and legal environment, health care providers must be far more rigorous when entering into vendor relationships in which patient-identifiable information will be placed at risk. The recently enacted HITECH Act provisions of the American Recovery and Reinvestment Act strengthen the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations. For the first time, providers have a mandate to notify patients of security breaches that involve their information. Specifically, the HITECH Act requires providers to notify patients of security breaches of "unsecured" patient-identifiable information, defined and referred to as protected health information (PHI).

Shortly after issuance of the HITECH Act, the Department of Health and Human Services (HHS) published a guidance document[2] indicating that PHI can be properly "secured" if it is encrypted or destroyed in accordance with HHS guidance. If PHI is "secured," then it is not subject to the security breach notification requirements. However, it is virtually impossible to maintain PHI in an encrypted state when it is in "use" (i.e., being created, viewed, modified, etc). As a result and from a practical perspective, at any given moment, providers will have significant PHI at risk of a security breach that will trigger the notification requirements.

Health care providers frequently hire vendors, referred to as business associates (BAs), to perform services involving PHI, including services that require the BA to create, view, or modify PHI. Such PHI is also subject to the HITECH Act security breach notification requirements. However, if a BA has a security breach that triggers the notification requirements, that BA's sole obligation under the HITECH Act is to notify the provider. The obligation to notify affected patients and to take other required action remains with the provider. There could be

significant costs associated with security breach notification, including (but not limited to) the cost of creating and sending out the required notifications and responding to queries and complaints from affected patients, as well as the costs to implement mitigation steps, such as free credit report monitoring. Costs may also be associated with negative publicity and governmental investigation and enforcement action. Absent contractual provisions that address allocation of liability for costs associated with security breach notification requirements, a provider will likely find itself liable for all costs connected to security breaches of PHI that was under the control of a BA.

HIPAA and the HITECH Act contain requirements that providers must follow when contracting with BAs, including contractually binding their BAs to implement security measures to protect PHI. However, providers are not legally required to monitor a BA's contractual or statutory compliance with HIPAA and the HITECH Act. Although BAs are directly subject to the HIPAA Security Rule under the HITECH Act, as noted above, much of the risk and liability associated with security breaches remains with the providers. Therefore, in this new environment, providers should take a more regimented approach to security to further mitigate risk. The recommendations in this article are intended to reduce the likelihood of security breaches by ensuring that BAs are obligated to provide "best practice" protections for handling PHI.

Reducing information security threats

Providers have three tools they can immediately put to use to substantially reduce the information security threats posed by their BAs, ensure proper due diligence is conducted and documented, and provide remedies in the event of a compromise.

Those tools are:

- the due diligence questionnaire,
- key contractual protections, and
- the use in appropriate circumstances of an Information Security Requirements exhibit.

Whenever a BA will have access to an organization's network, facilities, PHI, or other sensitive or valuable data, one or more of these tools should be used.

Use of these tools will enable a provider to achieve a number of important goals, including:

- **Reduce risk of security breaches** that trigger notification requirements under the HITECH Act and minimize potential liability. As noted above, costs arising out of security breaches and associated with security breach notification can be substantial. In addition to investigations by government agencies of HHS, security breaches could result in actions by state attorneys general.
- **Protect valuable assets of the provider.** In many instances, a provider's proprietary and confidential information is the most important asset of the company (e.g., new service lines, future marketing activities, prospective transactions, trade secret information, computer source code). Such information in the hands of a competitor could result in material harm for the provider. For publicly traded providers, a compromise of corporate data may result in shareholder suits against the officers of the corporation for failure to exercise reasonable business judgment in protecting that information.
- **Create contractual remedies for providers** in the event of a security breach with a BA.
- **Establish the provider has used due diligence in protecting PHI** and its information systems. In the event of a compromise, the tools will assist the provider in documenting its efforts to minimize risk.
- **Protect the provider's reputation** and avoid the public embarrassment associated with a security compromise.

Due diligence: The first tool

Providers may conduct some form of due diligence before entrusting BAs with PHI or with access to their systems. However, the due diligence is often done informally, in a non-uniform manner, and not clearly documented. In very few instances is the outcome of that due diligence actually incorporated into the parties' contract. This ad hoc approach to due diligence may no longer be appropriate or reasonable in the context of today's business and regulatory environment. To help ensure proper documentation and uniformity of the due diligence process, especially for high risk arrangements, providers should consider developing a standard "due diligence questionnaire" for prospective BAs to complete. Areas covered by the questionnaire would include: corporate responsibility, insurance coverage, financial condition, personnel practices, information security policies, physical security, logical security, disaster recovery and business continuity, and other relevant areas.

Use of a standardized questionnaire has a number of significant benefits:

- It provides a uniform, ready-made framework for due diligence.
- It ensures an "apples-to-apples" comparison of BA responses.
- It ensures all key areas of diligence are addressed and none are overlooked.

Continued on page 34

 ...continued from page 33

- It provides an easy means of incorporating the due diligence information directly into the party's contract. That is, the completed questionnaire can be attached as an exhibit to the final BA agreement, which will be executed along with the underlying services agreement.

From the outset, BAs must be on notice that the information they provide as part of the due diligence process and, in particular, in response to the due diligence questionnaire will be (1) relied upon in selecting the BA; and (2) incorporated into and made a part of the final BA agreement, together with the underlying services agreement between the parties. To be most effective, the questionnaire should be presented to potential BAs at the earliest possible stage in the relationship. It should be included as part of all relevant RFPs or, if no RFP is issued, as a stand-alone document during preliminary discussions with the BA.

Key areas for the due diligence questionnaire include:

- **BA's financial condition.** Is the BA a private or public company? Can the provider obtain copies of the most recent financial statements? Financial condition may not appear to be a critical factor for information security purposes, but the possibility a BA may file bankruptcy or simply cease to do business while in possession of a provider's most sensitive information presents a substantial risk, especially in today's current economic environment. In such instances, it may be difficult, if not impossible, to retrieve the data and ensure it has been properly scrubbed from the BA's information systems.
- **Insurance coverages.** What types of coverage does the BA have? What are the coverage limits and other terms? Is the coverage "claims made" or "occurrence based"? Does the BA's insurance cover liability related to privacy violations or security breaches?
- **Corporate responsibility.** Are there any criminal convictions, recent material litigation, or instances in which the BA has had a substantial compromise of security? Has it ever been investigated for privacy violations, etc.?
- **Subcontractors or affiliates.** Will the BA use subcontractors or affiliates in the performance of its services? Will the BA use subcontractors or affiliates outside the United States? Where are the subcontractors and affiliates located? What types of services will they provide? What information, if any, of the provider will be sent to these entities? Transmission of PHI to contractors or subcontractors located outside the United States has been identified as creating unique risk. Such entities will not be subject to US court jurisdiction. There have been highly publicized reports of situations where

PHI was potentially subject to unauthorized disclosure, including an instance in which a non–US-based contractor threatened to publish the PHI if it did not receive payments.

- **Organizational security procedures.** What are the BA's information handling policies? Does it have a dedicated information security team? Is there an incident response team? What are the BA's information security practices with contractors and agents (e.g., due diligence, requiring non-disclosure agreements, specific contractual obligations relating to information security)?
- **Physical security.** What physical security measures and procedures does the BA employ?
- **Encryption.** Does the BA use appropriate encryption technologies to protect PHI and other sensitive information?
- **Document destruction.** Does the BA destroy PHI and other sensitive information through appropriate methods, such as shredding paper, film or other hard copies, and clearing, purging or destroying electronic media in accordance with HIPAA requirements?
- **Audit trail.** Does the BA have appropriate access controls and logging/audit trail capabilities?
- **System access control.** Does the BA use system access control to limit information access to only those of its personnel who are specifically authorized?
- **Development and maintenance of code.** If the BA is a software developer, what are its development and maintenance procedures? What security controls are used during the development lifecycle? Does BA conduct security testing of its software? Does the BA maintain separate environments for testing and production? Does the BA license code from third parties for incorporation into its products? If so, what types of code?
- **Security policy and privacy policy.** If PHI is at risk, does the BA have an information security policy and privacy policy? What is the revision history of its policies? Are there any instances where the BA has had to contact patients or consumers regarding a breach of security?
- **Disaster recovery.** What are the BA's business continuity/disaster recovery plans? When was its last test? When was its last audit? Were there any adverse findings in the audit? Have deficiencies been corrected? What is the revision history of its plan? What security procedures are followed at the recovery site?
- **Red Flag Rules.** Does the BA have an identity theft program designed to identify, detect, and respond to Red Flags (see Title 16 of the Code of Federal Regulations Part 681)? What is their process for notifying providers of potential Red Flags?

Key contractual protections: The second tool

In the overwhelming majority of engagements, the underlying services contract entered into between a provider and its BAs has little or no specific language relating to information security. At most, a passing reference is made to undefined security requirements set forth in the BA agreement and a basic confidentiality clause. Of course, the BA agreement should contain language requiring the BA to "implement reasonable and appropriate administrative, physical, and technical safeguards to protect the confidentiality, availability, and integrity" of PHI. However, today's best practices in BA contracting suggest far more specific language is required.

Moreover, the personnel responsible for negotiating the underlying services agreement are often not those charged with negotiating the BA agreement. As a result, there is often a disconnect between the risks to PHI implicated by the types of contemplated services and the terms to protect such PHI, as well to protect the provider, in the BA agreement. Providers should consider inserting very specific language into underlying agreements, referencing information security provisions in the BA agreement, and clearly incorporating such agreement into the underlying services agreement. The underlying services agreement and the BA agreement should be read together to ensure that ambiguities related to information security are eliminated (e.g., confidentiality provisions in the underlying agreement that could be interpreted to apply to PHI, which conflict with the terms of the BA agreement).

Providers had until February, 2010 to amend their BA agreements to include language required under the HITECH Act. This presented a critical opportunity to more specifically address information security. In addition to other provisions that must be inserted under the HITECH Act, the following protections related to information security should be considered for inclusion in relevant BA agreements.

Warranties

In addition to any standard warranties relating to how the services are to be performed and authority to enter into the underlying services agreement, the following specific warranties relating to information security should be considered for BA agreements:

- A warranty requiring the BA to comply with "best industry practices relating to information security;"
- Compliance with the provider's privacy policy in accessing, using, and disclosing PHI;
- A warranty against sending PHI to offshore subcontractors or affiliates, unless specifically authorized to do so by the provider; and

Continued on page 36

- A warranty stating that the BA's responses are true and correct, for those arrangements in which the due diligence questionnaire has been completed. A copy of the completed questionnaire should be attached as an exhibit to the contract.

Information security obligations

In addition to the provisions relating to the BA's compliance with the HIPAA Security Rule, and generalized language relating to the BA's obligations to take all reasonable measures to prevent unauthorized uses or disclosures of PHI and to report all breaches or potential breaches of security to the provider, consider addressing more specific information security obligations. Consider, where appropriate, inserting specific language requiring the BA to:

- secure and defend its information systems and facilities from unauthorized access or intrusion,
- participate in joint security audits,
- periodically test its systems and facilities for vulnerabilities,
- use appropriate encryption and access control technology where applicable, and
- use proper methods and techniques for destruction of PHI to render such PHI "secure," as set forth in the HHS guidance.

Indemnity

Consider including with general indemnity language, a specific provision requiring the BA to hold the provider harmless from claims, damages, and expenses incurred by the provider that result from a breach of the BA's security. That is, the BA should protect the provider from lawsuits and other claims that result from the BA's failure to adequately secure its systems. In the past, indemnity provisions were often negotiated out of BA agreements. However, in light of the heightened enforcement environment (including the authority conferred upon state attorneys general to bring civil actions against providers), decisions to forego indemnification should be reevaluated for risk under each BA arrangement.

Costs for security breach notification

As noted above, there could be significant costs associated with security breach notification, including costs related making the required notification, as well as costs associated with negative publicity and governmental investigation and enforcement action. Consider inserting provisions into the BA agreement that require the BA to pay for all costs associated with security breach notification requirements, if a security breach occurs with PHI in the control of the BA.

Other provisions

In addition to the BA agreement, other provisions impacting information security in the underlying services agreement should be evaluated as follows.

Limitation of liability

Most software/services agreements, and many other services agreements have some form of "limitation of liability" (i.e., a provision designed to limit the type and extent of damages to which the contracting parties may be exposed). It is not uncommon to see these provisions disclaim the BA's liability for all consequential damages (e.g., lost profits, harm to the provider's reputation) and limit all other liability to some fraction of the fees paid. These types of provisions are almost impossible to remove from most underlying services agreements, but it is possible to require the BA to exclude from the limitations those damages flowing from the BA's breach of the BA agreement, including breaches related to information security obligations. Without these exclusions, the contractual protections described above would be essentially illusory. If the BA has no real liability for breach of privacy or confidentiality, because the limitation of liability limits the damages the BA must pay to a negligible amount, the providers contractual protections are rendered meaningless.

Confidentiality

The BA agreement is the venue for protecting the privacy and security of PHI. However, a fully-fleshed out confidentiality clause should be the cornerstone for information security protections related to non-PHI in every underlying services agreement. The confidentiality clause should be broadly drafted to include all information the provider desires to be held in confidence. Specific examples of protected information should be included (e.g., source code, proprietary care plans, marketing plans, new product information, trade secrets, financial information). Although the term of confidentiality protection may be fixed (for, say, five years), ongoing perpetual protection should be expressly provided for valuable information, such as trade secrets of the provider. Requirements that the provider mark relevant information as "confidential" or "proprietary" should be avoided. These types of requirements are unrealistic in the context of most arrangements. The parties frequently neglect to comply with these requirements, resulting in proprietary, confidential information being placed at risk. It will be important to read the confidentiality provision carefully in conjunction with the protections for PHI under the BA agreement to ensure there is no ambiguity.

Information security requirements exhibit: The third tool

The final tool in minimizing BA information security risks is the use of an exhibit or statement of work to specifically define the security requirements relevant for a particular transaction. For example, engagements in which PHI or other highly sensitive information will be entrusted to a BA may require the BA to observe strict practices in its handling of the information.

For example, the information security requirements exhibit may prohibit the BA from transmitting the provider's information over internal wireless networks (e.g., 802.11a/b/g) or from transferring that information to removable media (e.g., flash drives, CDs) that could be easily misplaced or lost. The exhibit may also contain specific requirements for use of encryption and access control technology, and decommissioning hardware and storage media on which the provider's information was stored. These measures ensure that the information is properly scrubbed from the hardware and media. Other specific physical and logical security measures should be identified as relevant to the particular transaction.

Conclusion

Providers are presented with unique risks when they entrust PHI and their proprietary and confidential information to their BAs. Those risks can be minimized by employing the tools discussed in this article: appropriate and uniform due diligence, use of specific contractual protections relating to information security, and use (where relevant) of exhibits or other attachments to the agreement detailing unique security requirements to be imposed on the BA. ■

1 Available at www.ponemon.org/news-2/23
2 74 Fed. Reg. 19006 (April 27, 2009). This guidance was updated and reissued as part of the Interim Final Rule on the HITECH Act security breach notification requirements, Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42740, 4271 (August 24, 2009).