HIPAA Cyber Security: Your Vendor is a Back Door to Your Server

Prepared for the American Health Lawyers Association's
Fraud and Compliance Forum held October 6, 2014

John E. Kelly, Esq.
Member
Bass, Berry & Sims PLC
Washington, DC

Nesrin Garan Tift, Esq.
Associate
Bass, Berry & Sims, PLC
Nashville, TN

I. Introduction

Providers and other healthcare organizations are increasingly finding themselves on the hook for their vendors' security incidents and missteps affecting electronic patient information. A security lapse by a vendor makes the provider potentially liable for federal and state notification obligations, which can result in monetary and reputational losses, and it also opens the door for government investigation and inquiry into the provider's own compliance with information privacy and security requirements. Further, modifications to the federal privacy rules and recent government enforcement suggest a duty on the part of the provider or company to assess the sufficiency of the vendor's security program initially and on an ongoing basis, as well as to take corrective action when deficiencies are identified. In short, if a government investigation resulting from a vendor's breach uncovers the provider's insufficient due diligence or lack of internal compliance measures, what may have started as the *vendor's* error promptly becomes the *provider's* problem.

The escalation in government enforcement of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[1] is evident from a review of recent actions by the Office for Civil Rights ("OCR"), which include investigations under increasingly stringent standards for regulatory compliance and imposing record penalties. At the same time that government enforcement of HIPAA increases, health information technology ("HIT") platforms have become an attractive target for hackers and other cybercriminals, particularly due to the value of "big data" found in the healthcare industry. A high-profile data breach announced in August, 2014, in which the records of nearly 4.5 million patients of hospitals owned by a large health system were stolen by hackers, has made the industry and consumers acutely aware of this threat, highlighting that cybercriminals are becoming more sophisticated and are increasingly able to go undetected. This rise in targeted activity, amidst the heightened government enforcement efforts and looming 2014 HIPAA compliance audits, is forcing healthcare organizations to take a closer look at the security of their databases and their procedures for managing risks to patient information. Further compounding these risks is the fact that the business of healthcare is increasingly dependent on healthcare data exchange and system interoperability, in turn prompting providers and health plans to outsource HIT functions to third-party vendors. Notably, OCR's actions send a clear message to providers, health plans and other healthcare entities

that they cannot simply turn a blind eye when entrusting their patient information and related systems to the cybersecurity of their vendors.

This paper provides guidance on the risks that a covered entity or business associate assumes when contracting with a vendor that has access to, transmits, or stores protected health information ("PHI") on behalf of the company. It begins by addressing how regulatory changes have impacted business associates' relationships to the government and to their contracting clients, causing those throughout the healthcare industry to re-examine their relationships and increasing risk exposure for both healthcare organizations and their vendors. It also examines the potential consequences of outsourcing HIT functions to a vendor and the resulting obligations, investigations and other legal action that may arise solely due to a vendor's security missteps. It demonstrates how these risks may be compounded by an entity's failure to oversee its vendors' security practices, or to merely take a passive role in monitoring the vendor's activities. Lastly, it provides strategies for healthcare companies to mitigate and re-allocate these risks so as to avoid hefty fines and government scrutiny.

II. Background

Statutory and regulatory changes in the last several years have transformed the course of HIPAA compliance and enforcement. In 2009, the Health Information Technology for Economic and Clinical Health Act ("HITECH")[2] made sweeping changes to HIPAA, notably granting OCR more substantial tools for taking action against HIPAA violations, creating a federal obligation to report a breach affecting patient information, and making changes to the role of business associates and their relationships with covered entities. In January of 2013, OCR released the long-awaited Omnibus Final Rule to implement modifications to HIPAA under HITECH (the "Omnibus Rule"), as well as to further strengthen the privacy and security protections for patient information.[3]

A. *Business Associate relationships after HITECH and the Omnibus Rule*

In the wake of the Omnibus Rule's changes, healthcare companies have struggled with the question of when a business associate agreement ("BAA") is required with a vendor or other contracting party. This determination has increasingly significant consequences in the new regulatory landscape. Failure to memorialize a business associate relationship with a vendor that handles PHI can create compliance risks, both as a potential violation of the requirement to implement a BAA prior to disclosing PHI to the vendor, and also with respect to the entity's lack of contractual protections from the vendor's mishandling of PHI. In 2012, OCR made waves by going after a small cardiology practice owned by just two physicians, requiring the practice to pay $100,000 to settle allegations of HIPAA violations.[4] The settlement followed a breach that arose when a vendor of the practice, an Internet-based email and calendar service provider, caused patient appointments and information to be posted online. Upon investigation, OCR cited not the vendor's actions but rather the practice's lack of HIPAA policies and procedures, focusing on its failure to obtain satisfactory assurances of the vendor's protection of PHI through a BAA.

At a basic level, a business associate relationship exists when a vendor provides services for or on behalf of a covered entity (or business associate) that involve the disclosure of PHI to the vendor.[5] The mere selling of healthcare items and services does not deem the vendor a business associate, provided the vendor does not access or use PHI to perform its functions. On the other hand, a vendor that requires access to PHI, such as a software company that accesses PHI for troubleshooting and other support services offered under the contract, is a business associate. Notably, the Omnibus Rule expanded the definition of a business associate to expressly include an entity that *maintains* PHI, "even if the entity does not actually view the [PHI]," and an entity that *transmits* PHI (unless that entity merely has "random and infrequent" access to PHI), in connection with a function covered by the Privacy Rule.[6] Further, the Omnibus Rule extended the scope of business associates to include subcontractors that provide services to business associates, to the extent they require access to PHI to perform such service. These changes have prompted covered entities and business associates to re-examine their vendor relationships and to seek contractual protections from any vendor that accesses, or has the opportunity to access, PHI on a routine basis.[7]

A word of caution -- entering into a BAA with a vendor when the parties' relationship does *not* create a business associate arrangement may unnecessarily ascribe liability on both sides of the arrangement. In response to the Omnibus Rule and recent, high profile data breach-related OCR settlements, a number of covered entities have taken well-intentioned but misinformed steps to execute a BAA with any party with which the company contracts. For example, a hospital system fearing a high profile HIPAA breach may ask a laboratory company, with which it contracts for the provision of diagnostic testing to the hospital's patients, to sign a BAA to obtain written assurance of the lab's HIPAA compliance and to provide contractual protections for the hospital in the event of the lab's breach. However, both providers should be aware that such an agreement is not appropriate where the exchange of PHI is for treatment purposes only.[8] Implementing BAAs across the board as an attempt to demonstrate HIPAA compliance does not benefit either party as it may give rise to liability on both sides, as discussed more fully below. Therefore, the determination of the parties' roles should be carefully considered at the beginning of any contractual relationship.

B. *Covered entity liability for the acts of an agent*

Often covered entities ask, if OCR can now go after a business associate directly for a HIPAA violation, why do I remain at risk for my vendors' breaches or missteps? While HITECH ascribed direct liability to business associates for violating certain privacy and security obligations under HIPAA,[9] covered entities are not free of risk for their business associates' acts. In fact, the Omnibus Rule expanded a covered entity's liability for the acts or omissions of its business associates, to the extent that vendor is acting as its agent.

Under HIPAA, a covered entity is liable for the acts or omissions of an agent, including a business associate, acting within the scope of such agency.[10] Significantly, the Omnibus Rule removed an exception that sheltered a covered entity from direct liability for

a vendor's HIPAA violation if the parties had in place a compliant BAA and the covered entity had no knowledge of, and did not fail to act upon, the vendor's breach of the BAA.[11] In effect, when a provider delegates an obligation under HIPAA to a business associate, such provider may be held liable for the business associate's failure to perform such obligation, regardless of whether the parties have a compliant BAA in place. Further, a provider's lack of knowledge about a business associate's HIPAA violations is no longer a partial defense to liability.

Following this change, those in the healthcare industry have been left to question the degree of risk they assume for their vendors, due in part to a lack of certainty as to when a business associate or subcontractor is acting as an "agent" and what actions are within the scope of that agency. OCR declined to define these terms in favor of a fact-specific determination that turns on "the right or authority of a covered entity to control the business associate's conduct."[12] Where each party has contractual obligations with respect to a particular function, the business associate would not likely be acting as the covered entity's agent. On the other hand, where a covered entity has the authority to direct or control how the business associate will carry out a particular function after the parties' relationship has been established, the business associate would likely be considered the agent of the covered entity.

To the extent a healthcare organization delegates HIPAA obligations to a vendor, such as providing patients access to their medical records upon request, the organization may be held liable for the vendor's failure to sufficiently perform such obligation. Further, when the vendor has access to or maintains the covered entity's PHI on a server or electronic database, this risk is arguably increased. In the event of a lapse or misstep by a vendor affecting the security of such PHI, the covered entity could be liable not only for the notification obligations triggered by a breach, but also for any penalty imposed by OCR for a violation caused by the vendor's acts.

III. Vendor's security breach: consequences for the covered entity or business associate

Among other significant modifications to the privacy and security obligations under HIPAA, HITECH introduced a federal reporting obligation in the event of a breach of unsecured PHI.[13] While a business associate is required to notify the covered entity in the event of a breach caused by the business associate, the covered entity must notify affected individuals, the U.S. Department of Health & Human Services ("HHS"), and in cases of a breach affecting more than 500 individuals, the media.[14] Therefore, even in the event a vendor is the sole cause of a breach affecting patient information, the covered entity bears the responsibility for notifying affected parties, as well as liability for failure to meet any of the prescribed timing, content and manner of reporting rules. Further, beyond the financial burdens of reporting, the covered entity is exposed to reputational losses as well; through patient communications, media releases (if required) and other public awareness. The covered entity remains the "face" of the breach despite any third parties' acts.

However, occasionally the parties may seek to shift the responsibility for individual notifications to the business associate through contractual negotiations. Both parties may see advantages to this delegation: the business associate retains some control of communications made to affected individuals, and the covered entity shifts costs of notification to the vendor. However, delegating this obligation can lead to uncertainties with respect to the breach response, investigation and mitigation responsibilities, and may even expose the covered entity to increased risk. For example, if the parties undertake independent risk assessments to determine whether a breach occurred,[15] they may reach conflicting conclusions leading to possible disputes regarding notification responsibilities. Further, if a business associate assumes responsibility for preparing and sending breach notification letters and other communications, the covered entity may wish to retain the right to review and approve any materials. The parties should also consider the requirement to provide contact information for individuals seeking information about the breach,[16] and should determine which party retains responsibility for addressing inquiries. Lastly, delegating this obligation to notify affected individuals in the event of a breach may, in the event of a dispute or investigation, cause a court or OCR to view the vendor as the covered entity's agent, thereby exposing the entity to increased risk as discussed above.

As the incidence of criminal activity and other lapses in cybersecurity continue to affect the HIT sector, revealing growing risks to patient data, covered entities and business associates should take care to negotiate and be transparent about the parties' roles in allowing the affected covered entity to meet its breach obligations. This should include, if necessary, specifying procedures in the event the parties disagree about whether a breach occurred, allocating the costs of preparing notifications, and stating whether one party has a right to review and approve communications prepared by the notifying party.

IV. Consequences beyond the breach

The consequences of a vendor's security lapse potentially extend beyond the costs of mitigating and responding to a breach, and it could expose a covered entity or business associate to government investigation and/or class action litigation.

A. *OCR investigation: risk assessment as a critical step in avoiding penalties*

OCR will open a compliance review to investigate any reported breach of unsecured PHI affecting 500 or more individuals, and has the discretion to do the same with respect to a breach affecting fewer than 500 individuals. In January, 2013, OCR announced the first settlement in connection with a breach affecting fewer than 500 patients when the Hospice of North Idaho was required to pay $50,000 in connection with the 2010 theft of an unencrypted laptop containing PHI of 441 patients.[17] During the investigation, OCR discovered that the hospice workforce routinely used portable laptops to conduct fieldwork. However, the hospice had failed to conduct a risk analysis to identify threats to the security of electronic PHI maintained on the laptops, and accordingly did not implement measures sufficient to protect the PHI. This case was noteworthy in signaling that no breach is too small and no lapse too insignificant to avoid OCR action.

While the occurrence of a breach alone may not give rise to penalties under HIPAA, failing to conduct a security risk analysis may make penalties more likely if OCR determines that the entity failed to assess or act upon known security threats. As demonstrated above, the lack of a documented risk analysis is a recurring theme in many recent OCR enforcement actions, revealing this as a potential weakness in HIPAA compliance across a broad spectrum of healthcare organizations. For example, OCR reached a record $4.8 million settlement in May of this year against two health system providers when a security lapse allowed the PHI of roughly 6,800 patients to become accessible through internet search engines.[18] OCR's investigation found that the entities had not sufficiently performed a risk analysis to determine weaknesses in their HIT applications and databases, and further failed to implement security measures sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level. Many healthcare companies subject to HIPAA seem to lack a clear understanding of what a risk analysis requires, as well as its significance in demonstrating HIPAA compliance and potentially avoiding the imposition of penalties.[19]

OCR has provided guidance on the significance of a risk analysis, stating that it "form[s] the foundation upon which an entity's necessary security activities are built."[20] A risk analysis involves conducting an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI on an entity's system.[21] It requires identifying potential threats to electronic PHI, assessing the entity's current security measures, determining the likelihood and criticality of potential threats, and finally implementing security measures sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level. In addition, the risk analysis is a continuous process, necessitating review and updates to security measures whenever new technologies are introduced or in light of operational, environmental and regulatory changes.[22]

However, when faced with OCR investigation following a breach, having a documented risk analysis does not shield the entity from liability if the entity failed to act upon such analysis. OCR has demonstrated that it will hold covered entities and business associates responsible for failure to implement protective measures in response to known threats. For example, in 2014, OCR reached a $1.73 million settlement with Concentra Health Services following the report of a breach involving a stolen, unencrypted laptop containing patient information.[23] As noted by OCR, Concentra had documented through multiple risk analyses that PHI was vulnerable to threats based on a lack of encryption on company laptops. However, Concentra had not taken sufficient measures to reduce this threat by completing the encryption process across all company laptops at the time of the breach.[24]

In the event of a breach or complaint leading to an investigation by OCR, it is a near certainty that OCR will request a copy of the entity's most recent risk analysis. In addition, if the incident was caused by or related to a vendor's actions, OCR may be likely to seek documentation that the covered entity assessed the *vendor's* systems and processes as part of its risk analysis to determine the threats to electronic PHI stored on the vendor's server (or resulting from a vendor's access to the covered entity's system). Moreover, OCR may

seek evidence that the covered entity implemented measures to reduce identified threats to an appropriate level.

B. *Other types of exposure*

Even assuming OCR declines to open a compliance review following a breach, or does open a compliance review but declines to impose penalties, a covered entity (or business associate) may face exposure to liability based on a vendor's actions or omissions through other legal processes including HIPAA compliance audits and costly private litigation.

1. HIPAA compliance audits

HITECH required OCR to perform periodic audits assessing covered entities' and business associates' compliance with the privacy and security obligations of HIPAA.[25] Under OCR's audit pilot program, which was completed in late 2012, an entity subject to an audit received a broad request for documentation relating to HIPAA, including policies and procedures, and was subject to a site visit between 3 and 10 business days in length.[26] OCR would then provide an audit report summarizing its findings, allowing the audited entity 10 days to review the report and describe corrective actions taken to address any identified issues. OCR has indicated that the audits serve primarily as a compliance improvement activity. However, if an audit indicates a serious compliance issue, OCR may initiate a separate compliance review or investigation. In other words, the audited entity may find itself facing investigation and potential penalties if the audit reveals deficiencies.

While the pilot program audited 115 covered entities, OCR has indicated that the second round of audits, slated to being in the Fall of 2014, will cover about 350 covered entities as well as 50 business associates. The results from the first round of audits revealed that the security rule accounted for the majority of deficiencies discovered. As a result, healthcare organizations should expect an increased focus on security rule compliance including the use of encryption methodologies and procedures for authorizing and monitoring access to systems containing electronic PHI.[27]

Given the increased scope of the upcoming second round of audits, as well as OCR's pointed concern with security rule compliance, healthcare organizations subject to HIPAA should consider this the time to take a closer look at their internal program relating to information privacy and security, as well as their vendors' compliance with respect to any outsourced HIT functions. Amidst the current press around cyber attacks and large-scale breaches of patient information, there is the potential that OCR takes this opportunity to closely assess the cybersecurity of audited entities, including surveying their practices around authorizing access to information systems containing PHI and monitoring vendor safeguards to protect patient data.

2. Class action litigation

Although HIPAA does not provide a private right of action, recent case law demonstrates that a breach or other incident affecting patient information can potentially

serve as grounds for a common law claim, which in some instances has opened the door to class action litigation.

In *Tabata v. Charleston Area Medical Center,* the West Virginia Supreme Court of Appeals held that patients had standing to bring a cause of action against a hospital for breach of confidentiality caused by the hospital's breach of PHI and further reversed the lower court's ruling that the patients failed to meet the requirements for class certification.[28] In 2011, over 3,600 patients of a West Virginia hospital received notice of a breach occurring when a database operated by the hospital was accidently placed on the Internet. The database contained the patients' clinical information, names, social security numbers, and dates of birth. The named plaintiffs filed an action in state court alleging that the hospital breached its duty of confidentiality, and also sought class certification. The circuit court ruled the plaintiffs lacked standing to sue and denied class certification. Notably, discovery in this case did not reveal that any patients' medical records or personal information had been accessed by an unauthorized person, and further determined that plaintiffs had "not suffered any property injuries or sustained any actual economic losses."[29] On appeal, however, the West Virginia Supreme Court of Appeals disagreed with the lower court's ruling, finding the plaintiffs had a legal interest in having their medical information protected and further that they met the requirements for class certification. Though the court conceded the patients had suffered no economic or property injury, it determined that the hospital's breach gave rise to a cause of action under common law for a violation of the patients' right to the privacy of their medical information.[30] Similarly, in March, 2014, Stanford University Hospital & Clinics and two of its vendors agreed to a settlement of a class action lawsuit, requiring them to pay over $4.1 million in total to settle claims in connection with a data breach that caused personal information of roughly 20,000 emergency room patients to be accessible on the Internet for nearly one year.[31] Notably, in this case, the hospital was not found in violation of any legal requirements by federal and state agencies, and the breach was caused solely by the hospital's vendor. Regardless, the hospital bore significant losses in connection with the settlement in order to avoid the costs of ongoing litigation.

V. Strategies for mitigating risk

With each hacking incident, attention is drawn to the healthcare industry's vulnerability to cyber attacks, sending a clear message that it can happen to anyone. Healthcare organizations can take important steps to mitigate the risk of a breach, as well as to ensure that if a breach does occur, they are in the best position possible to address and respond to government investigation or other legal action. Further, healthcare organizations should focus due inquiry into their vendors' security practices, both at the start of and throughout the relationship, as OCR will not absolve them of liability for a violation due to the fault of a vendor. The following is a summary of recommended strategies for covered entities and business associates to mitigate risks posed by their vendors who store or transmit PHI on their behalf.

First, health care companies should track all vendor relationships to determine whether a business associate relationship is created, remaining careful not to hold a vendor

out as one's business associate if not appropriate as this could subject both parties to unwarranted liability. Where a BAA is appropriate, the agreement should clearly delineate the parties' respective responsibilities (and related costs) concerning a breach affecting patient information. Further, despite the lack of distinct guidance from OCR on what determines an agency relationship, the takeaway is clear: covered entities and business associates must be aware that they potentially take on increased risk exposure due to the acts and omissions of their business associates. A covered entity or business associate may wish to reconsider the terms of its vendor agreements (such as the degree of control the entity maintains over the vendor's obligations) so as to avoid a determination of agency, where feasible.

Second, covered entities and business associates should consider strategies to reallocate risks through contractual negotiation. Entities may seek indemnification from their vendors for any breach of unsecured PHI or, more broadly, any violation of HIPAA or the BAA. Further, such contracting entity should consider any limitation of liability provisions in a service agreement or BAA that could potentially affect its right to seek indemnification. Lastly, entities should also consider requiring vendors to maintain cyber liability insurance to cover a breach that would trigger liability for the entity.

Third, actions by OCR and the targeted cyber attacks on the healthcare industry demand that healthcare organizations maintain a heightened level of oversight of vendors controlling, maintaining or having access to a server containing patient information. However, the demand for oversight does not require a one-size-fits all approach. Instead, entities may need to prioritize certain vendors based on factors such as the nature and amount of PHI the vendor has access to, the criticality of the vendor's functions, and any known deficiencies in the vendor's security program. Further, vendor oversight should be performed on an initial and ongoing basis. As one method of oversight, health plans and other organizations may require a vendor to provide a written attestation regarding its security program and/or to sign a security compliance agreement separate and apart from the BAA. Others are adopting a more stringent approach, involving on-site reviews and periodic attestations.

An organization's chosen method of vendor risk management, along with the degree to which an entity monitors its vendors, should be considered carefully. A covered entity that knows of a business associate's breach of its HIPAA obligations, but does not take steps to end the breach or, if not possible, terminate the contract, is in violation of HIPAA.[32] Further, as demonstrated by recent enforcement actions, if an investigation reveals that the covered entity was aware of deficiencies or vulnerabilities in the vendor's cybersecurity practices, but continued to use such vendor for a function involving access to PHI, OCR may be more likely to impose penalties despite the covered entity's lack of fault in causing the breach. Healthcare organizations should maintain a clear process and procedure for evaluating and responding to its awareness of vendors' practices and missteps, including and up to termination of the contract.

Fourth, organizations should also integrate vendor oversight into their overall HIPAA compliance plan. For example, the security rule requires an entity to implement

access controls to ensure that only authorized users are permitted access to systems containing PHI, as well as to regularly review information system activity, such as audit logs and access reports.[33] Vendor risk management should be incorporated into these existing practices. For example, before contracting with a vendor that will have access to an electronic database containing PHI, an entity should consider the extent to which its authentication controls and system activity reports may be extended to the vendor. Will the entity be able to track the vendor's access to and use of the system? If the vendor maintains its own server or network containing the entity's PHI, should the entity request and review the vendor's access reports and audit logs? Integrating vendors into an entity's compliance plan can help to identify and mitigate risk factors due to vendor operations.

Finally, beyond oversight of a vendor's HIPAA compliance, one of the most important steps for mitigating risk is focusing on a company's own internal privacy and security procedures. As we have seen, a breach or other incident affecting patient information (even when seemingly caused by no fault of the covered entity) opens the door to possible government investigation, thereby potentially exposing gaps in the investigated entity's HIPAA program. Further, the second round of HIPAA audits is imminent and will reach a wider range of healthcare entities, aimed at identifying and correcting deficiencies in organizations' compliance with HIPAA. As evidenced by OCR's initial audit findings, many organizations lack an awareness of their obligations under the security rule (in particular, the significance of a risk analysis). Conducting a HIPAA gap analysis and implementing corrective action when necessary can help mitigate the risk of enforcement following a breach, as well as help to foster a culture of compliance with HIPAA privacy and security. While vendor risk management can prove a challenge, organizations are encouraged to maintain awareness of their vendors' acts and to integrate vendors into their existing policies and procedures. Doing so can help protect the organization from known, as well as unknown, threats to patient data.

---

[1] Pub. L. 104-191 (August 21, 1996).
[2] Pub. L. 111-5 (Feb. 17, 2009).
[3] 78 Fed. Reg. 5566 (January 25, 2013).
[4] The Resolution Agreement between OCR and Phoenix Cardiac Surgery can be found at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf.
[5] 45 C.F.R. § 160.103.
[6] *See* 78 Fed. Reg. at 5571-2.
[7] *Id*.
[8] *See* 45 C.F.R. § 160.103 (excluding from the definition of "business associate" a health care provider, "with respect to disclosures by a covered entity to the healthcare provider concerning the treatment of the individual").
[9] *See* Pub. L. 111-5, § 13401.
[10] 45 C.F.R. § 160.402.
[11] *See* 78 Fed. Reg. at 5581.
[12] *Id.* at 5582.
[13] *See* Pub. L. 111-5, § 13400; implementing regulations set forth at 45 C.F.R. Part 164, Subpart D.
[14] 45 C.F.R. §§ 164.404-410.
[15] *See* 45 C.F.R. § 164.402 for the definition of a "Breach."
[16] 45 C.F.R. § 164.404(c)(1)(E).

[17] Press release, *HHS announces first HIPAA breach settlement involving less than 500 patients* (January 2, 2013), available at http://www.hhs.gov/news/press/2013pres/01/20130102a.html.
[18] Press release, *Data breach results in $4.8 million HIPAA settlements* (May 7, 2014), available at http://www.hhs.gov/news/press/2014pres/05/20140507b.html.
[19] *See* "HIPAA Privacy, Security and Breach Notification Audits," presented by OCR at the HCCA 2013 Compliance Institute on April 23, 2013.
[20] *HIPAA Security Standards: Administrative Safeguards* , available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf ; see also *Guidance on risk analysis requirements under the HIPAA Security Rule* (July 14, 2010), available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalintro.html.
[21] 45 C.F.R. § 164.308(a)(1)(ii)(A).
[22] *See* 45 C.F.R. §§ 164.306(e), 164.316(b)(iii).
[23] Press release, *Stolen laptops lead to important HIPAA settlements* (April 22, 2014), available at http://www.hhs.gov/news/press/2014pres/04/20140422b.html.
[24] The Resolution Agreement is available at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/stolenlaptops-agreements.html.
[25] Pub. L. 111-5, § 13411.
[26] The Audit Pilot Program is described at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/auditpilotprogram.html.
[27] *See* "HIPAA Privacy, Security and Breach Notification Audits," presented by OCR at the HCCA 2013 Compliance Institute on April 23, 2013.
[28] 759 S.E. 2d 459 (W. Va. 2014).
[29] *Id.* at 463.
[30] *Id.* at 464.
[31] *Springer v. Stanford Hosps. And Clinics*, Cal. Super. Ct., No. BC470522.
[32] 45 C.F.R. 164.504(e)(1)(ii).
[33] *See* 45 C.F.R. 164.308(a)(1)(i)(D), 164.312(a)(1).