HIPAA Enforcement Gets Serious—Are You Ready?

Susan Huntington, Esq.
Counsel, Day Pitney LLP, Hartford, Connecticut

James ("Jim") Bowers, Esq.
Senior Counsel, Day Pitney LLP, Hartford, Connecticut

Eric Fader, Esq.
Counsel, Day Pitney LLP, New York, New York

Background

Data breaches affecting the healthcare industry have reached epidemic proportions. Over the past two years massive breaches affecting millions of individuals have been legion involving Anthem, Premera, Community Health Systems, Triple S Management Services, University of California, Los Angeles Health, Excellus Health Plan, Medical Informatics Engineering and 21st Century Oncology. Correspondingly, the number of breaches reported to the Office for Civil Rights (OCR) of the Department of Health and Human Services (HHS), which enforces the Health Insurance Portability and Accountability Act (HIPAA) keeps growing. OCR lists more than 80 reported breaches involving 500 or more individuals1 in just the first four months of 2016,2 including covered entities such as hospitals, physicians and health plans along with business associates including a law firm, a gas and electric company and a benefit plan.

The healthcare industry’s migration to increasing dependence on digital technologies, including electronic health records, population management programs, data analytics and cloud-based computing, continues to create significant exposure for unauthorized access to or release of vast amounts of electronic protected health information (ePHI). Cyberattacks are certain to continue given the accelerated use of electronic applications and reliance on digitalized information.

While mega healthcare data breaches likely involve sophisticated hacking by organizations from global locations like China and North Korea, most breaches continue to be the result of theft or loss of laptops, portable electronic devices or other electronic media containing unsecured ePHI. Regardless of whether a situation involves intentional unauthorized access to digital systems in order to steal ePHI or negligent loss of devices that contains ePHI, it is still a breach and, therefore, a likely violation of HIPAA.

Until recently, the OCR had not been very aggressive in its enforcement actions against covered entities. This fact was noted in an audit report released in September 2015 in which HHS’s Office of Inspector General (OIG) found that OCR had been less than effective in its enforcement of the HIPAA Privacy Rule. OCR accepted OIG’s audit finding and undertook to resume HIPAA compliance audits, which began in March 2016. Also, OCR has become increasingly aggressive in bringing enforcement actions when ePHI has been compromised through

---

1 Since the implementation of the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, covered entities under HIPAA are required to report to patients as well as OCR (and often to state regulators) any breach that involves 500 or more individuals in a single state or jurisdiction, and are also required to issue a press release.

data breaches. Regulatory fines have consistently been in the million dollar range and enforcement is likely to increase now that OCR has resumed its HIPAA compliance audits.

**Recent OCR Enforcement Activities**

OCR significantly increased its visibility through aggressive privacy enforcement in 2016, having brought six actions since the beginning of the year. Four of these have been announced since mid-March, with the latest announcement that New York Presbyterian had agreed to pay $2.2 million to resolve claims that it violated HIPAA by disclosing two patients’ health information to ABC personnel during the filming of the documentary television series *NY Med*. This resolution followed a $750,000 settlement with Raleigh Orthopaedic Clinic, P.A. for allegedly failing to execute a required business associate agreement (BAA), a $3.9 million deal to resolve a claim that The Feinstein Institute for Medical Research did not have proper privacy and security procedures in place, and a $1.5 million settlement to address allegations that North Memorial Health Care System disclosed patient data to a major contractor without a BAA.

Although the government has been stressing the importance of BAAs since the HITECH Act was released in 2009, some covered entities still haven’t executed BAAs with all of their business associates, and other covered entities haven’t updated their existing BAAs to comply with changes that were mandated by the 2013 HIPAA Omnibus Rule. So any healthcare provider or business associate that assumes that its BAA executed several years ago puts it in compliance with HIPAA’s current BAA requirements is likely mistaken.

**OCR’s Phase 2 Audits**

In March, OCR announced the commencement of its long-awaited Phase 2 HIPAA compliance audits. The Phase 2 audit targets cover individual and organizational providers, health plans of all sizes and functions and a range of business associates of these entities. The majority of the audits will consist of remote desk reviews, although some onsite reviews will take place. If the audits uncover serious compliance issues, further investigations may occur, with the potential imposition of penalties and corrective action plans.

OCR has indicated through its updated audit protocol that a main focus of the audits will be confirming that all necessary BAAs are in place and they meet current requirements. Therefore, failure to have all required BAAs in place could very well be considered an inherently serious violation with possible fines or penalties, given the core importance of BAAs under HIPAA.

Unfortunately, even if a covered entity or business associate is lucky enough not to be chosen for an OCR audit, it is not out of the woods. When (not if) a breach occurs, the spotlight will be focused on key compliance elements of HIPAA.

**Breach May be Inevitable—Are You Ready for the Spotlight?**

In their investigations of breaches, OCR and state regulators generally first seek to confirm the presence of basic privacy and security safeguards they consider fundamental. These items have been requirements for over a decade, so OCR and state regulators will likely show little mercy when they are not in place:

- privacy and security awareness training of employees;
- policies and procedures;
- security risk analyses and risk management plans;
- intrusion detection and firewalls;
- encryption of mobile devices; and
- business associate agreements and vendor management.

If these controls are not in place, a company will find itself in a defensive position from the outset.

**Elements of an Effective HIPAA Privacy and Security Program**

Cybersecurity is a business risk, not purely a technology risk, and needs to be managed on an enterprise-wide basis to include people, process and technology. Healthcare data breaches are usually caused by a combination of control failures (involving, e.g., patch management, incident response, network perimeter monitoring and employee training) at healthcare entities that result in compromising the privacy and security of ePHI. The remediation needed to address those control failures is the implementation of a comprehensive data privacy and secu-

---

3 One example is a 2016 settlement announced by the Connecticut Attorney General, in which a hospital and its business associate, an international information technology company, agreed to pay a $90,000 fine and agreed to changes in its policies and procedures following a breach in which the required BAA was not in place. See [http://www.ct.gov/ag/lib/ag/press_releases/2015/20151105_hartford_hospital_privacyavenue.pdf](http://www.ct.gov/ag/lib/ag/press_releases/2015/20151105_hartford_hospital_privacyavenue.pdf)
A risk assessment should examine the administrative, physical and technical controls for safeguarding ePHI. Areas that would need to be assessed include: (i) policies and procedures relating to workforce security, access, security incidents and contingency planning; (ii) training on such policies and procedures; (iii) facility access controls, workstation use and security, device and media controls; (iv) transmission security (encryption), person and entity authentication and integrity controls (to prevent alteration and destruction); and (v) vendor privacy and security assessments and safeguards. The assessment of the sufficiency of vendor privacy and security safeguards is critical given the amount of healthcare data accessed by vendors and the fact that a substantial percentage of healthcare data breaches have resulted from poor vendor security controls.

Cybersecurity risk assessment processes are now encouraged or mandated by many federal and state regulators. First and foremost, a security risk assessment is required under the HIPAA Audit Program Protocol. In its pilot HIPAA audits conducted during 2011-2012, OCR found that a major deficiency was the failure to conduct a security risk assessment to identify and mitigate risks to ePHI. These risk areas included ePHI on exposed servers, laptops unencrypted, default passwords not changed, security software not up to date and inadequate security training.

I Know I Need to be Prepared, but Where to Start?

Since healthcare data breaches have become daily occurrences, healthcare entities and their business associates should not be penny-wise and pound-foolish in strengthening their privacy and security control environments. Based on its...
annual benchmark study of healthcare organizations, the respected Ponemon Institute has determined that the costs associated with a data breach have continued to increase to an average of $2.35 million in 2015. Therefore, it is prudent to dedicate adequate resources to build an effective cybersecurity compliance program rather than bearing the expenses resulting from a data breach, which can include expenses for breach notification and credit monitoring, legal advice, forensic investigation, data repair/replacement, business interruption, regulatory fines and penalties and civil lawsuits—not to mention the adverse impact on reputation.

Implementing compliance controls can be overwhelming. Where should an organization start? Focus on where OCR and state regulators focus:

1. Perform Risk Assessment

As previously discussed, the most common deficiency found by OCR in its pilot audits was an organization’s failure to conduct a security risk assessment to identify and mitigate risks to ePHI. This deficiency continues to be found in recent OCR enforcement actions. Accordingly, this area of noncompliance should be the primary focus for both covered entities and business associates. While these risk assessments can be very in-depth, they don’t have to be overly complicated. For example, Day Pitney LLP has developed a HIPAA Self-Assessment Tool based on OCR’s audit protocol to assist covered entities and business associates in performing a risk assessment.5

2. Update Business Associate Agreements

OCR and state regulators have no tolerance for the absence of BAAs between covered entities and their vendors. Every covered entity should review its existing relationships with business associates to ensure that an up-to-date BAA that complies with HIPAA requirements has been executed.

3. Adequate Employee Training

Ensure that employee training contains the most current HIPAA requirements. Consider having enhanced training for those employees who have more access to and handle PHI such as data analysts, medical records personnel and clinicians. Be sure to maintain records that document employee training on at least an annual basis.

4. Develop an Incident Response Plan

Organizations need to be able to act quickly in the event of a data breach. An incident response plan enables a company to handle data incidents efficiently, thereby minimizing damage to the company in the event of a data breach. A well-executed response plan will facilitate the validation, investigation and mitigation of a data breach and ensure timely notification of regulators and affected individuals.

Conclusion

This article is intended to provide a blueprint for managing HIPAA compliance exposure. As noted, a HIPAA compliance program should be tailored to the size, complexity, core activities and corresponding data security risks faced by an organization. It is critical that a HIPAA risk assessment be conducted to determine what components should be a part of the organization’s compliance program. Of course, an organization should always seek legal advice if there are questions about the sufficiency of the privacy and security compliance program it is implementing or updating. ☛

"The HIPAA Journal noted that Day Pitney’s HIPAA Self-Assessment Tool was useful and simple to use, http://www.hipajournal.com/day-pitney-launches-new-hipaa-self-assessment-tool-ahead-of-compliance-audits-8218/". For more information, contact one of the authors through the email address provided.