ALERT
NOVEMBER 16, 2012

HEALTH LAW
News Concerning
Recent Health Law Issues

COZEN O'CONNOR

HIPAA Enforcement – The Gathering Storm Has Arrived

Gregory M. Fliszar • 215.665.7276 • *gfliszar@cozen.com*

Since the Health Insurance Portability and Accountability Act (HIPAA) privacy rules became effective in April 2003, there has been minimal enforcement activity by the U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR). However, this has changed dramatically over the last two years, as evidenced by some recent high-profile and high-penalty enforcement actions taken by OCR. In addition to being concerned about OCR investigations, covered entities and business associates must also be on the alert for enforcement actions by state attorney generals, potential class action lawsuits, and OCR's HIPAA audit program. Even though many in the health care industry are sitting in a holding pattern waiting for the HIPAA/Health Information Technology for Economic and Clinical Health (HITECH) Act final rules, covered entities and business associates should thus be as vigilant as ever, if not more so, in their HIPAA compliance efforts.

1. OCR Enforcement

Over the last two years OCR has significantly increased its HIPAA enforcement efforts. Following an extensive investigation by OCR, Massachusetts General Hospital agreed in February 2011 to pay the U.S. government $1,000,000 and enter into a corrective action plan to settle potential HIPAA violations. The incident giving rise to the agreement involved the loss of protected health information (PHI) of 192 infectious disease patients, including those with HIV/AIDS, that occurred when a hospital employee left the records on a subway car (the resolution agreement can be found here. In addition, on March 13, 2012 BlueCross BlueShield of Tennessee (BCBST) agreed to pay the government a $1.5 million civil penalty and enter into a corrective action plan, following an investigation by OCR into a breach reported by BCBST pursuant to the breach notification provisions of the HITECH Act. Despite having a number of security measures in place, 57 hard drives containing the PHI of more than 1 million individuals were stolen from a BCBST-leased facility (the resolution agreement can be found here). The enforcement action was the first resulting from a report made under the HITECH Act breach notification provisions and implementing regulations. See 42 C.F.R. § 164.400 *et seq*. More recently, OCR concluded another investigation resulting from a HITECH Act breach notification. On September 17, 2012 Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc. (MEEI) agreed to pay the U.S. government $1.5 million to settle potential HIPAA violations, enter into a corrective action plan, and retain an independent monitor to report on MEEI's compliance efforts. The breach report and subsequent OCR investigation resulted from the theft of a single laptop containing the unencrypted electronic PHI of over 3,600 MEEI patients and research subjects (the resolution agreement can be found here).

2. State Attorney General Investigation

State attorney generals have also exercised the authority vested in them by the HITECH Act to bring civil actions on behalf of state residents for violations of HIPAA. *See* 42 U.S.C. § 17939(e). Connecticut was the first state to pursue actions for HIPAA violations under HITECH Act's new enforcement authority bringing a case against insurer Health Net. Inc. for waiting six months to provide notification of a lost computer disk drive that contained unencrypted PHI, social security numbers and bank account information for nearly 500,000 Connecticut enrollees. Health Net ultimately agreed to pay $250,000 in penalties. Vermont residents were also affected by the same Health Net data breach, and its attorney general pursued its own actions against Health Net, resulting in Health Net paying a penalty of $55,000 and agreeing to data security audits. More recently, in May of 2012, Massachusetts announced that its attorney general settled a lawsuit against South Shore Hospital for $750,000 to resolve alleged HIPAA and consumer protections violations resulting from a data breach involving unencrypted backup computer tapes. In another groundbreaking action, on July 30, 2012 the Minnesota Attorney General announced that it had settled its lawsuit against business associate Accretive Health, Inc. The attorney general alleged violations of HIPAA, which stemmed from a stolen laptop containing PHI, and state unfair debt collections practices. *See* Minnesota attorney general press release here. Under the combined settlement Accretive agreed to pay nearly $ 2.5 million to the state of Minnesota and refrain from conducting business in the state for six years (although it could request permission to return in two years).

3. Class Action Lawsuits

Although HIPAA includes no private right of action, individuals who have had their PHI lost, stolen or inappropriately accessed have begun to bring their own lawsuits based on data breaches – namely class action lawsuits against covered entities for alleged failure to adequately protect the individuals' PHI. For example, the UCLA Health System is the defendant in a class action lawsuit seeking approximately $16 million, following a data breach that occurred when a hard drive was stolen from the home of a former UCLA physician that contained the PHI of more than 16,000 patients. The class action lawsuit was brought not under HIPAA, but the California Confidentiality of Medical Information Act, which, like HIPAA, prohibits health care providers from disclosing patient data without consent unless the disclosure is otherwise permitted or required by law. Similarly, a lawsuit was filed against a Georgia hospital in June of this year following a data breach that included the loss of unencrypted PHI of more than 300,000 patients (*Bombardieri v. Emory Healthcare, Inc.*, Ga. Super. Ct. No. 2112cv2/5883, filed 6/4/2012). The complaint again alleged numerous state law causes of action, but stated HIPAA imposed industry standards and duties with which the hospital failed to comply.

Some recent court decisions have dismissed claims by plaintiffs in data breach cases, based on a finding that the threat of future harm from such a breach is not enough to show the plaintiff suffered an injury that would sustain a claim against defendants; there must be actual use of the information by a third party causing harm. *See e.g. Paul v. Providence Health System-Oregon*, 273 P.3d 106 (Or. 2012). Thus, a breach itself was not actionable without evidence the plaintiff was damaged by the inappropriate use of the information breached.

Nevertheless, once a covered entity reports a breach to HHS and the breach is posted on the HHS website, the entity should not only prepare for a possible OCR investigation into the breach, but also take into account the chance of a potential class action lawsuit as well.

4. OCR HIPAA Audits.

HHS has also begun to move forward with its auditing of HIPAA compliance. The HITECH Act requires the Secretary of HHS to provide for "periodic audits" of covered entities and business associates to assess their compliance with the HIPAA privacy and security rules and the HITECH beach notification provisions. 42 U.S.C. § 17940. In response to this mandate, OCR piloted a program to perform 115 audits of covered entities beginning in November 2011 and scheduled to conclude in December 2012, with the permanent audit program to follow thereafter. OCR states the covered entities it has chosen to audit represent a wide range of health care providers, health plans and health care clearinghouses. The factors OCR considers when selecting an audit target include the type of entity, where the entity is located, whether the entity is public or private, the size of the entity, affiliation with other health care organizations, and past and present interactions with OCR regarding HIPAA enforcement and breach notification. OCR has hinted that although it will be planning for audits of business associates in 2013, those audits might not take place until 2014, possibly due to the fact that the final rules on business associates have not yet been released.

In June of this year, OCR finally posted its HIPAA audit protocol, which can be found here. The protocol includes separate sections for assessing compliance with the privacy rule, the security rule and breach notification. It includes 78 performance criteria for assessing compliance with the privacy rule, 77 criteria for assessing compliance with the security rule, and 10 criteria for assessing compliance with breach notification that will be reviewed during on-site visits lasting several days. Notably, OCR has stated any audits that reveal significant noncompliance with HIPAA's requirements could prompt an investigation by OCR.

The new HIPAA audit program is, therefore, yet one more avenue for the government to enforce HIPAA and the HITECH Act. The audit process itself would be difficult for most any covered entity to endure, yet findings of noncompliance may also result in enhanced enforcement consequences. Further, business associates, and possibly even their subcontractors, may also soon become targets of OCR's audit program.

5. Conclusion

After years of minimal HIPAA enforcement, covered entities and business associates are now being bombarded by increased enforcement actions coming from a number of different directions. As a result, a single breach of PHI can have devastating consequences. For example, a hospital employee might decide to do some work at home and download patient files onto an unencrypted jump drive, which he puts into his backpack. If the backpack is mistakenly left on a chair at a coffee shop and eventually stolen, the hospital now has a breach on its hands. If it is determined the breach must be reported to HHS, it is possible the hospital may be subject to an investigation by OCR and possibly even the state attorney general. If the breach was large enough to be posted on the HHS website, a plaintiffs' attorney could target the hospital for a class action lawsuit that must now be defended. Finally, the mandated report to OCR resulting from the breach might cause the hospital to be a more attractive candidate for a HIPAA audit.

Covered entities and business associates must remain vigilant in their HIPAA compliance efforts. This includes, without limitation, conducting thorough risk assessments, developing and updating robust HIPAA policies and procedures, and conducting ongoing HIPAA training and awareness programs with all staff. In essence, affected entities must create what OCR has often referred to as a "culture of compliance." Moreover, emphasis should be placed on the use and safeguards of portable electronic devices, which are frequently at the center of a data breach.

To discuss any questions you may have regarding HIPAA and/or HITECH, or how they may apply to your particular circumstances, please contact:

Gregory M. Fliszar at gfliszar@cozen.com or 215.665.7276

Katherine M. Layman at klayman@cozen.com or 215.665.2746

For additional news and analysis on health law issues, subscribe to our blog Health Law Informer.