wiley

ARTICLE

HIPAA Enforcement May Finally Be Getting Tougher

Health Care Law360
April 20, 2012

With its most recent enforcement effort, the U.S. Department of Health and Human Services (HHS) may finally have signaled the beginning of a new enforcement era for Health Insurance Portability and Accountability Act (HIPAA) privacy and security violations.

With the final HIPAA/Health Information Technology for Economic and Clinical Health (HITECH) Act regulations slowly making their way through the final steps toward approval and publication, it is critical for health care companies and their business partners to monitor their HIPAA compliance efforts, particularly on the security front and to act quickly in the event of a problem or an open investigation.

Enforcement Background

While many, including this author, assumed that HIPAA enforcement would grow during the early stages of the Obama administration — driven both by a new administration more focused on privacy issues than its predecessor had been and the new penalty opportunities provided by the HITECH statute — that new enforcement era has been very slow in coming. Only very limited steps have been taken, even today.

The Office of Civil Rights (OCR) action against Cignet Health of Prince George's County, Md., initially seemed to be an important step, but it quickly became clear that the penalty in that case was based largely on Cignet's utter failure to make any reasonable effort to comply with HIPAA or to cooperate in any way with the OCR investigation.

Practice Areas

D&O and Financial Institution Liability
Health Care
Privacy, Cyber & Data Governance

Accordingly, that action was essentially one to be disregarded, unless a company has chosen to completely ignore a government investigation, not a strategy I typically recommend. The Massachusetts General Hospital case, involving documents left on a subway by a facility employee, seemed much more "typical," but it stood alone and therefore was not reasonably viewed as the start of a trend.

The Minnesota attorney general has created a parallel enforcement concern, through a recent action initiated against a HIPAA business associate that is not even yet subject to HHS enforcement, but that case is so far the only outlier from an attorney general, aside from some "routine" and infrequent security cases.

The Tennessee Case

Now, OCR has issued a new penalty, in a significant case involving Blue Cross Blue Shield of Tennessee. This case, while still one of a small number of enforcement actions, seems to be more of an indicator of what we are likely to see in the future than any of the previous HIPAA actions. Accordingly, it is an important matter for any company in the health care industry and all business partners to understand and monitor.

The Tennessee case stands out for several reasons. The basic facts are straightforward.

In October of 2009, Blue Cross Blue Shield of Tennessee (BCBSTN) discovered that computer equipment had been stolen from an office location it was leasing. The stolen equipment included 57 hard drives containing electronic data. The hard drives had been placed in this location in connection with a significant office move.

BCBSTN's internal investigation determined that protected health information involving 1,023,209 individuals had been stored on the hard drives, including member names, social security numbers, diagnosis codes, dates of birth and health plan identification numbers.

BCBSTN notified individuals and HHS, along with the media, as required by the HITECH breach notification regulation. The OCR settlement does not challenge BCBSTN's compliance with this breach-notification standard in any way.

The case, therefore, becomes important because it is the first matter that was brought to OCR's attention through an appropriate breach-notification disclosure, and an enforcement action resulted not from defects in that notification but from a subsequent investigation of BCBSTN's security practices resulting from the notification.

During its investigation following the breach notification, OCR's investigation determined, from OCR's perspective, that BCBSTN had failed to meet the requirements of the HIPAA security rule, by failing to implement appropriate administrative safeguards to adequately protect information remaining at the leased facility where the hard drives were stolen, by not performing the required security evaluation in response to operational changes as a result of the office move.

Also, OCR determined that BCBSTN had failed to implement appropriate physical safeguards by not having adequate facility access controls. As a result of these findings, BCBSTN agreed to pay $1.5 million to settle the OCR allegations that it violated the HIPAA security rule.

In addition, BCBSTN agreed to a corrective action plan to address and resolve its purported security problems. As part of the settlement, BCBSTN has agreed to a variety of new steps, including obligations to

- Review, revise and maintain its privacy and security policies and procedures;
- Conduct "regular and robust" trainings for all BCBSTN employees covering employee responsibilities under HIPAA; and
- Perform monitor reviews to ensure the company's compliance with the corrective action plan.

Implications

This case leads to several important conclusions for health care companies and their business partners going forward.

First, while compliance with the breach notification rule obviously is important, complying with this rule does not mean that a company will avoid enforcement action. In fact, one could draw the conclusion that a company is likely to face a significant investigation into its practices as a result of a breach notification.

Second, the OCR review of security practices will be strict and comprehensive, even if these investigations are not fast. We are seeing a broader range of investigative requests related to security practices and documentation, both in "normal" complaint investigations, in connection with reported breaches, and in connection with the ongoing HIPAA audit program. Because security breaches remain common and widespread in the health care industry, this is a significant area for concern.

Third, companies should learn from the mistakes of their peers — and pay close attention to any lessons that can be learned from every enforcement action. The Mass General case teaches companies to have better controls over their paper records. The Tennessee case is an important reminder of what can go wrong in connection with office moves. So, use these actions to improve and verify your own practices.

Fourth, if a breach is being investigated in your company and notification is likely, it is critical that companies review their security practices at the same time as the breach is being investigated. You should expect an investigation to follow a reported breach. As the Tennessee case indicates, this follow-on investigation may not occur quickly, but it likely will occur.

Fifth, the HHS is beefing up its corrective action plans, with substantial details on security practices and ongoing obligations that will be very burdensome. While the HHS agreements do not yet mirror the efforts of some other privacy enforcement actions, such as the 20-year compliance obligations ordered in typical settlements by the Federal Trade Commission, these continuing obligations — with ongoing monitoring and oversight — are quite significant.

Sixth, this case is yet another reminder of the importance of strong overall security practices, whether you are a covered entity, a HIPAA business associate or a downstream contractor of a business associate. Business associates and subcontractors, in particular, should be paying close attention to their overall security practices, because these entities quickly will be facing new compliance obligations to follow the full HIPAA Security Rule when the HITECH regulations are finalized.

Covered entities, presumably, have been in compliance for several years, but this case — and many others in the news, even without enforcement activities — indicates that ongoing security vigilance is essential for the health care industry today.

Business associates should begin moving toward full HIPAA compliance now, because modifications likely needed to meet security rule obligations do not happen quickly, and the substance of the security rule provisions will not be changing in the final regulations.