COSMOS
Navigate the Compliance Universe

Compliance Today - June 2024

Daniel F. Shay (dshay@gosfield.com, linkedin.com/in/daniel-shay-a65039a3/) is an Attorney at Alice G. Gosfield & Associates P.C. in Philadelphia, PA.

An inside view of HIPAA enforcement

by Daniel F. Shay

While many healthcare providers are generally aware of their obligations under HIPAA, most do not have a clear sense of what happens if they fail to meet these obligations. At best, most probably are familiar with headlines about healthcare providers entering into multimillion-dollar settlements with the government for HIPAA violations but otherwise may be unaware of the specifics of such cases. In an environment where, for example, cybersecurity incidents are increasingly common, it can be nerve-wracking for healthcare providers to contemplate actually meeting their HIPAA obligations in the face of such ongoing threats—especially while the specter of enormous HIPAA penalties looms large in their minds. This article is intended to pull back the curtain on how HIPAA violations actually play out and help illustrate ways healthcare providers may mitigate or even avoid HIPAA penalties.

An in-depth case study

In the summer of 2016, a client of our firm became aware of a hacking incident on its server that had originated overseas. The client was a small physician practice that, at the time, housed its server on-site and utilized a local IT professional to provide ongoing electronic security and support services. The hack itself occurred over several days (until it was discovered), and the client notified the U.S. Department of Health and Human Services Office for Civil Rights (OCR)—the government entity responsible for HIPAA enforcement—of the incident a few days later. During the hack, the client's electronic medical records software was encrypted and locked and thus unavailable to the client.

The client's situation was, to put it mildly, problematic. At the time of the hack, although the client had some administrative, physical, and technical safeguards in place, most of its HIPAA Security Rule compliance had been handed to the lone IT support person who did not know or understand the requirements of HIPAA very well. The server in question was also not as physically secure as it could have been. It was located in its own room but with an unlocked door. Moreover, the cables connected to the server had been configured improperly for the network router, and the effectiveness of the client's firewall device had been reduced (improperly) to correct a network connectivity issue. Antivirus and antimalware software likewise were not functioning properly; they had not been kept up to date, and the IT professional had not been performing daily scans, even though their contract required them to do so. In addition, the client's HIPAA security risk assessment had not been updated in years and was sparse at best. Moreover, the client used a published book to train its staff rather than draft its own policies and procedures.

However, the client's extensive remedial steps were cutting in its favor. First, the client instructed its electronic health records (EHRs) software vendor to investigate the problem and restore access. Then, the client hired an outside auditor to investigate what had gone wrong internally. The client then fired the IT professional it had

been using and hired a new company with actual HIPAA experience; the client later demanded a return of payments made to the previous IT professional for 2016.

In addition, the client hired a company to conduct a new security risk assessment and help it develop new policies and procedures, which would be updated periodically. It improved its physical security—including adding a door lock to its server room and installing security cameras on the building exterior. The client improved backup procedures, enabled screen lockouts, properly updated its software to the latest versions, and set up a separate guest Wi-Fi service to isolate personal devices on its network.

The client's report to OCR prompted an investigation, which led to the client bringing the matter to our firm. The client and I spent more than a month gathering evidence to demonstrate to OCR the good-faith efforts the client had made to comply with HIPAA. We outlined the remedial efforts the client had undertaken in response to the hack.

Fortunately, because the client had maintained extensive and contemporaneous documentation of its efforts, we were able to prepare a comprehensive narrative—supported by documentary evidence—to explain to OCR what had happened, what steps the client had taken, what matters were outside of its control or knowledge, and how the client had corrected the problems within its control. This included contemporaneous copies of emails sent to the IT professional and EHR software vendor, the policies and procedures that had been in place at the time of the hack, and the ones that replaced them (including a physical copy of the book the client had used). All this information was assembled both as physical copies and in electronic format on a USB thumb drive, with exhibits labeled for ease of reference. I hand-delivered all these materials to OCR's offices in March 2017.

OCR finally closed the case in December 2018; it imposed no penalties and required no remedial efforts from the client. Instead, it determined the client had voluntarily complied with HIPAA and provided minimal technical assistance as a guide for small medical practices. Beyond this, OCR determined the matter had been resolved.