PAUL HASTINGS

PH PERSPECTIVES

August 2015

Follow **@Paul_Hastings**

Three Lessons Learned from a Data Breach Investigation

By Behnam Dayanim & Mary-Elizabeth Hadley

As the number of data breaches continues to increase, so does the vigilance of regulatory authorities in investigating such incidents. In the healthcare industry, fines paid to resolve breaches of unsecured protected health information ("PHI") have grown to as high as $4.8 million. However, there are ways to avoid costly fines. Although far from a "sure thing," conducting a thorough, proactive investigation of the breach can convince the U.S. Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") to close the case without further action. If your company is in the unfortunate situation of a breach, we've provided some guidance that can help minimize your exposure.

These lessons learned were evidenced most recently in our Privacy and Cybersecurity Practice's successful non-monetary resolution of a recent hospital breach. Like many breaches, this one began with the theft of a laptop—a laptop that, in violation of hospital policies, included thousands of unencrypted patient records.

Here's what your company can learn from this success story:

Lesson #1: Take Immediate Action

Upon learning of the incident, the hospital swiftly launched a thorough internal investigation to determine which files and types of information may have been on the computer, what PHI may have been at risk of compromise, and which patients might be affected by the theft.

In compliance with the Health Insurance Portability and Accountability Act of 1996 and Health Information Technology for Economic and Clinical Health Act (collectively, "HIPAA"), the hospital notified patients whose PHI may have been compromised as well as the local media. The hospital also notified state authorities, as dictated by other laws. In addition, the hospital offered one year of identity theft protection to the notified data subjects and recommended they consider informing their banks, credit card companies and other financial institutions of the potential compromise. Finally, the hospital established a hotline and a "frequently asked questions" section on its website to assist data subjects with inquiries about the incident.

Equally as important, the hospital undertook a comprehensive external risk assessment of its policies and procedures in an effort to determine whether to make improvements that would reduce the risk of recurrence of this or similar incidents and more generally to consider whether other changes seemed warranted. The hospital engaged Paul Hastings to oversee both the breach investigation and the external risk assessment. Paul Hastings typically partners with forensics or similar consultants in

handling these types of matters, but retention of a law firm to direct the proceedings can ensure that attorney-client privilege is retained. It also allows the institution to determine carefully and, weighing all of the circumstances, whether and to what degree to share the results of the investigation with third party regulators.

Lesson #2: Assess and Address

In addition to security enhancements it had taken prior to the laptop theft—including acquisition of the ability to wipe data remotely from hospital-issued mobile devices, more consistent use of anti-virus and internet filtering software and installation of USB encryption agents on hospital computers—the hospital redoubled its commitment to information security following the incident. Notably, the hospital implemented a series of additional security improvements as a result of the findings of its risk assessment. Those improvements included: (i) an inventory of all devices capable of accessing ePHI and of hospital-issued laptops, (ii) installation of an email encryption service, (iii) deployment of software to encrypt USB drives that are used to download data from a hospital computer, (iv) encryption of backup tapes, (v) retention of a vendor for data destruction, and (vi) installation of software to increase visibility of remote access devices and guests.

The hospital also requires contractors to undergo hospital HIPAA training or to demonstrate adequate understanding of compliance through their company's own programs. Contractors must now also sign a statement acknowledging their understanding of the hospital's security policies and agreeing to comply with those policies.

Lesson #3: Be Open and Transparent

Both in its initial Breach Notification Report to HHS' OCR and its supplemental response, the hospital provided comprehensive information regarding the incident. The hospital candidly disclosed prior areas for improvement and detailed the strides it has made towards enhancing its privacy and data security controls. It also supplied OCR with all requested documentation, including relevant policies and procedures. Moreover, it anticipated requests OCR might make and supplied it with all information of potential relevance to the incident.

Implications for the Future

Six and seven figure HIPAA settlements will likely continue to grab headlines, but voluntary compliance actions such as a thorough internal investigation, an external risk assessment, and the implementation of security improvements can help to keep your company out of the headlines.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

San Francisco

Thomas P. Brown
1.415.856.7248
tombrown@paulhastings.com

Thomas A. Counts
1.415.856.7077
tomcounts@paulhastings.com

Paul M. Schwartz
1.415.856.7090
paulschwartz@paulhastings.com

Washington D.C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com

Mary-Elizabeth M. Hadley
1.202.551.1750
maryelizabethhadley@paulhastings.com