THE HIGH COST OF INACTION:
DATA BREACH, FINES AND TAKEAWAYS FOR THE HEALTHCARE INDUSTRY

As the Health Insurance Portability and Accountability Act (HIPAA) turns 20 years old this year, there are no signs of the law losing ground. To the contrary, according to the Office of Civil Rights (OCR) Director, Jocelyn Samuels, “OCR remains committed to strong enforcement of the HIPAA Rules.” (1) And the agency is not all bark. In fact, based on recent agency investigations, there is now even more bite behind the enforcement, providing a healthy reminder for the Healthcare industry to pay attention. With growing threats to patient privacy through online data breaches, now is the time for the Healthcare industry to recommit to compliance, especially related to data security measures, and to reexamine their insurance coverage to mitigate the costs of a potential breach.

The following summarizes just three recent investigations and the significant consequences as reported by the US. Department of Health & Human Services. (2)

CASE 1:
In November 2015, a large insurance holding company reported multiple breaches of its systems involving protected health information. After investigation, OCR found that the holding company had very little protection in place and was actually compounding the likelihood of information being compromised by offering more information than was necessary to business partners without securing protection agreements (Business Associate Agreements). As a result, the firm had to pay for the loss, implement corrective action and pay $3.5M in penalties. (1)

The Takeaway: The cost of not protecting information far exceeds the cost of taking appropriate security measures.

CASE 2:
In December 2015, a major research medical center was forced to provide corrective action and mitigate losses from an event where an employee from an affiliated organization downloaded malware that compromised the health information of 90,000 individuals. In addition, OCR levied a monetary penalty of $750,000 because the medical center failed to ensure that system-level risk assessments were completed and that corrective actions were taken by its affiliates as well. The assessment failed to include the whole system, including that of the affiliate. (2)

The Takeaway: Make sure that cyber security measures are implemented across the entire organization, including affiliates who have access to your valuable patient information.
CASE 3:
In August 2012, a medical group of 13 physicians were held responsible when an employee’s laptop was stolen from a car which contained the personal health information of 55,000 patients in an unencrypted format. In addition to the costs of the claim itself, OCR imposed a penalty of $750,000 due to the inadequate controls in place to protect the information.

The Takeaway: Controls must reach across all levels of the organization, including policies and procedures for employees. Data must be encrypted and electronic devices protected on and off site.

Protecting patient privacy is an essential responsibility within the industry. As demonstrated in the three cases above, even the most sophisticated medical providers have fallen short at times and paid the price. To remain compliant with HIPAA, it is imperative for Healthcare organizations to remain up-to-date on the latest threats to the data entrusted to them by their patients.

To learn more about how to protect your organization from a data breach, contact your Barney & Barney representative.

---

