THE
NATIONAL LAW REVIEW

Data Breaches Most Expensive For Health Care Industry But Precautionary Measures Can Keep Costs Down

Article By
Dena M. Castricone
Daniel J. Kagan
Murtha Cullina
Newsletters and Alerts

- Communications, Media & Internet
- Health Law & Managed Care

- All Federal

Wednesday, June 28, 2017

Data breaches have become commonplace in every industry. In health care, however, it costs much more to respond to a data breach than in all other industries in this country, according to the results of a recent IBM-sponsored study.[1] The report estimates that a health care data breach costs $380 per record on average versus $225 per record in other industries. While the increased cost of a health care record is unavoidable due to the sensitive nature of the information and the fact that it is more valuable to criminals on the dark web, health care providers can take steps to prepare for a data breach, which can reduce the risk of a breach occurring and minimize costs if one occurs.

First, be prepared. Entities should have a plan for responding to breaches that mobilizes an incident response team and identifies the most critical parties to contact: IT forensic vendor, legal counsel and your insurance broker. Health care providers and businesses will be best served by having an existing relationship with an IT vendor that can be available on a 24-hour basis to handle cyber security incidents; you do not want to be Googling "cyber security IT vendor" at 8 PM on a

Friday night after discovering a breach that cannot be managed internally. As for legal counsel, a skilled data breach lawyer will serve as the quarterback of the data breach response operation, determine legal obligations under various state and federal laws, offer attorney client privilege protection under certain circumstances and assist with a strategy to mitigate overall risk. Obviously, your insurance broker will help you access any available coverage your business may have (and you should have cyber liability coverage).

Second, comply with the HIPAA Security Rule. Many of the required measures under the HIPAA Security Rule will help reduce the risk of a breach of protected health information (PHI). Among other things, the rule calls for an assessment of all systems where PHI is stored, employee training on security and the implementation of policies and procedures that address the security of PHI and disaster recovery planning.

Finally, practice. We do fire drills because we want to be sure that people will know what to do in the event of a fire. The same is true of data breaches. Gather your incident response team and run through a breach scenario. Then, evaluate your plan to determine if it needs changes based on the results of the drill.

In today's world, all industries need to be prepared to respond to a data breach but given the increased risk and cost, health care providers need to move this item to the top of the list.

---

1 Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview, sponsored by IBM Security.

© Copyright 2019 Murtha Cullina

Source URL: https://www.natlawreview.com/article/data-breaches-most-expensive-health-care-industry-precautionary-measures-can-keep