Cost-Benefit Analysis 101 for Healthcare Providers

Prepared by:
Robert Laplaca
Verrill Dana, LLP

LORMAN®

Published on www.lorman.com - June 2018

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

Cost-Benefit Analysis 101 for Healthcare Providers

Written by Rosemary McKenna – 3/15/18

Nary a week goes by without news of a data breach by a healthcare provider…while there are certainly a good number of breaches resulting from a breach of cybersecurity defenses or from the wrongful exploitation of system security weaknesses, there is still a risk to healthcare providers resulting from the internal operations of the healthcare provider. There are frequent reports of these "internal" breaches: loss of equipment (e.g., laptops that were not secured and unencrypted USB drives), employee wrongdoing (e.g., theft of records or improper access to records to satisfy personal curiosity), and then those unfortunate "oops" moments (e.g., sending personal health information ("PHI") to administrative vendors without a proper business associate agreement ("BAA") in place, or a spontaneous conversation in a waiting room disclosing PHI).

Huge penalties are attached to these breaches. Healthcare entities (and their business associates) face stiff financial penalties: $150,000 for a lost, unencrypted flash drive, $750,000 for sending an administrative service provider

PHI without a signed BAA, and $2.5 million for a stolen laptop, just to name a few. These poor folks would also likely be required to implement corrective action plans for several years, internal and external costs of investigating the breach and navigating the U.S. Department of Health & Human Services Office for Civil Rights ("OCR") , and potential litigation, not to mention the adverse publicity. Let's not even get into the possibility of criminal penalties…

The Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act ("HIPAA/HITECH") requirements have been around for some time. These critical rules are being augmented by the regular passage of various state laws. Some enacted or proposed laws, such as the "Stop Hacks and Improve Electronic Data Security Act" ("SHIELD Act") legislation proposed by the NYS Attorney General, would not add requirements for companies who are in compliance with other cybersecurity laws such as HIPAA/HITECH. If you are not in compliance, however, then you could be facing OCR and other regulators as well.

Without doubt, many small or mid-sized healthcare providers have not complied with at least some of the security and privacy requirements under these laws as of this blog (please see monkey emojis above). We get it – healthcare payments are shrinking and compliance can be

a big nut – but ignoring compliance obligations gets more risky with each passing day.

If you need help meeting privacy requirements, are looking for assistance with HIPAA compliant policies and procedures or training, or if you have any questions, please let the Jackson Lewis Privacy, e-Communications and Data Security Practice Group know.