How to Prepare for a Data Breach in Healthcare

January 15, 2016

By Michael Reph and Ryan Roberts, Parker, Smith & Feek

To ensure proper data breach response preparedness (and to show proper due diligence), your directors and leadership staff should be asking I.T. and key partners the pertinent questions now, before a breach occurs:

- Have we ever had system penetration testing done, and have we reviewed the results?
  - -It is best to engage both your I.T. and compliance personnel to ensure any bad penetration results are remedied to their fullest extent possible. Understanding what a good outcome looks like is a starting point, with the end goal of surpassing those average outcomes.
- Do we have adequate I.T. security policies in place?
  - -Will these policies meet the burden of proof? You will have to demonstrate a consistent, defensible method for incident risk assessment to show due diligence and regulatory compliance. Adequate I.T. policies ensure that HIPAA requirements are met.
- Are we using updated operating systems to help manage electronic medical records?
  - -Out dated operating systems do not have the same encryption standards to comply with HIPAA regulatory requirements.
- Who would be working as our forensic team, post-breach?
  - -Most cyber insurance policies will provide for a dedicated forensic team, post-breach. Putting a cyber policy into place ensures that you have a team who will not only identify the key issue or type of event, but additionally, these policies help manage the breach ramifications for you, i.e. notifying all affected parties, engaging public relations professionals, managing lawsuits, and brand damage. Having someone manage this laborious and costly incident is well worth the cost of an insurance policy and corresponding deductible.
- Do we have a breach response plan in place?
  - -The fundamentals of a breach response plan consist of going through the steps listed above, staying up-to-date with the latest federal, state, and international and healthcare laws, and engaging appropriate outside partners such as outside counsel, an insurance broker, and breach response services to consult you on how to meet the varying requirements.
- Do we have sufficient cyber/data liability insurance coverage to mitigate the legal, reputational, and credit monitoring costs? And if we don't carry insurance coverage, will our current finances be sufficient to cover such costs when we have a data breach?
  - -A well-versed attorney or insurance broker who has handled cyber breach incidents can determine based on the number and type of healthcare records, the type of security measures, and the nature of the organization what sort of coverage would be sufficient. If an organization chooses to forgo insurance coverage, a "self insurance" ball park figure would be the average "consolidated total cost" (includes not just

immediate response costs but regulatory fines, lawsuits, customer churn, and brand damage): $3.79 million, according to the 015 Cost of a Data Breach Study by the Ponemon Institute.

Proper documentation of these internal conversations (via minutes) and actions (i.e. having readily available system penetration testing results and documenting the actions shoring up weaknesses) will help defend the organization in federal and civil lawsuits, post-breach. It is important to note that historical lawsuits have shown that directors are not required to be experts in this area, but that they do need to rely on outside experts or expert internal management for advice when addressing these issues. The Ponemon Institute indicates that 90% of healthcare organizations had exposed their patients' data or had it stolen in 2012 and 2013.

The ever-changing requirements in data breach notification requirements within the various state authorities and the federal law, continued increase in the number and severity of cyber attacks, and increase in the size of federal lawsuit judgments make this an important topic which needs to be addressed by healthcare organizations, both large and small. Partnering with a well-versed risk consultant in either a legal or insurance capacity who understands both the pre and post-cyber breach actions necessary to defend your organization will provide better organizational resiliency when your organization is attacked.

This paper was orginally published by The Northwest Regional Primary Care Association

http://www.nwrpca.org/news/269680/How-to-Prepare-for-a-Data-Breach-in-Healthcare.htm