Recent Cybersecurity Worries for Health Care Companies

PUBLISHED ON

October 10, 2018

October has already had a haunting effect on health care providers given the two big news stories related to compromised patient information.

The *Journal of the American Medical Association* recently released a staggering study regarding the recent data breaches that health care providers have been experiencing. The study reported that from 2010 through 2017, there were 2,149 data breaches reported by business associates, health plans and health care providers. Those breaches exposed 176.4 million records, according to the study.

While in 2010 the most common form of a breach was from a laptop or paper films, by 2017 the most common form of a breach was to network servers and emails. In 2017 alone, 132 million records cumulatively were breached due to hacking or an IT incident. The most common breach was through a health care provider, which accounted for 70 percent of the breaches. This study indicates that cyber hackers are targeting health care providers' networks and IT systems.

Hospital Employee Missteps

Then there was the recent $1 million settlement of three Boston hospitals related to potential HIPAA violations, proving there is a hefty price to pay when Protected Health Information (PHI) is not properly protected. This settlement arose from a compliance review investigation by the federal Office for Civil Rights after it learned that one Boston hospital was allowing ABC to film a documentary at the hospital.

The investigation revealed the hospital had impermissibly disclosed the PHI of patients to ABC employees during the filming of the documentary. Massachusetts General Hospital paid the stiffest fine of $515,000, Brigham Women's Hospital paid $384,000 and Boston Medical Care paid $40,000 in fines related to accusations from the Department of Health and Human Services and Office for Civil Rights for failure to appropriately and reasonably protect their patients' PHI from disclosure.

Although the results of the *JAMA* study show this type of employee-related compromise is on the downtrend when compared to incidences of network and IT breaches, the corrective action plans two of the three Boston hospitals agreed to complete are instructive since they can be molded to apply to network and IT breaches.

Making A Plan

The plans require the hospitals to develop processes, policies and procedures that:

- Address and evaluate HIPAA compliance

- Monitor access of PHI
- Provide internal reporting procedures to report and promptly investigate any violations of the hospitals' policies
- Identify agents or representative that employees can contact regarding HIPAA compliance
- Apply sanctions against employees that violate the hospitals' policies

The hospitals then must distribute the policies and train their employees on them. Any new employee must also receive the same training. The hospitals must also provide an implementation report that includes:

- A copy of all training materials
- Summary of employee violations of the new policies
- Confirmations by an owner or officer that the new policies are being implemented, employees have completed required training, the hospitals have complied with obligations of the plan, and that the report is truthful and accurate.

If a health care provider were to implement similar processes, policies, procedures and reporting related to protecting PHI from network and IT breaches, then this would be a beneficial initial defense that would likely help reduce the breadth of any breaches. It would also limit any hefty penalties that could arise from any breaches.

If you have any questions about the cybersecurity protection requirements, please contact me or any other member of the Barley Snyder Health Law Industry Group.

:

Elizabeth L. Melamed

Associate

Tel: 717-399-1538

Email: emelamed@barley.com