BURR FORMAN LLP

Cyber-Incident - Now What?

Articles / Publications
10.25.2018

Reprinted with Permission from the *Birmingham Medical News*.

In this day in age where a vast amount of information is stored electronically and you can buy almost anything with a "1-click" purchase, it comes as no surprise that cyber-incidents are on the rise, especially among healthcare providers. The attacks are becoming more and more sophisticated, thereby stumbling even the most savvy and educated employees. Thus, every health care provider should spend some time thinking about how to prepare for a cyber-attack and respond to a cyber-attack if one were to occur. In relation to cyber-attacks, I once heard someone say, it is not "if it will occur" but "when it will occur".

In order to prepare for an attack and perhaps reduce your exposure, below are a few steps that can be taken on the front end:

1. Put Together an Incident Response Team: Go ahead and put together an incident response team made up of members of your workforce and consultants that can assist with responding to an incident. Think about the people within your organization who have the authority to make decisions on behalf of the organization (e.g., President, Administrator, etc.), as things move very quickly once an incident occurs. Also think about the people within your organization who have expertise and experience that may be of value in response to an incident. For example, the Chief Security Officer or the HIPAA Privacy Officer. Finally, think about whether you want to include anyone from outside the organization on the team (e.g., your attorney) and go ahead and execute Business Associate Agreements with such persons.

RELATED PROFESSIONALS

Kelli Carpenter Fleming

Cyber-Incident - Now What?

2. Put a Plan in Place: Implement a plan addressing how to respond to a cyber-incident. Gather the input of you incident response team when drafting the plan. The plan should include such items as what security measures need to be implemented, how to back up the relevant data, who is responsible for certain tasks, how to contact members of the incident response team, and ways to preserve evidence and maintain documentation.
3. Review your Insurance Policy: As incidents continue to rise, several entities are now obtaining insurance policies that provide coverage for cyber-incidents. Further, some general liability policies may provide coverage for certain costs and expenses. Review the insurance policies you have in place to determine what is covered, how it is covered, and the steps that must be taken in order to obtain the coverage. For example, many policies do not provide coverage until the carrier is notified. As Previously mentioned, you have to move quickly in response to a cyber-incident, so knowing upfront that you need to first provide notice to your carrier will help move things forward. Some carriers also require that you use a specific law firm or specific forensics firm to address the incident.
4. Update Your Risk Assessment: HIPAA requires healthcare providers to conduct a risk analysis of their electronic systems to identify risk areas that may need to be addressed. It is important that your risk analysis incorporate all your systems and be up to date-a risk analysis from five years ago before you implemented an electronic health record is not sufficient. Not only is the risk analysis legally required, but it is also a good exercise to help determine your highest areas of risk so you can address those risk areas before an incident occurs.
5. Review and Update Your HIPAA Compliance Plan: In addition to security policies and protocols, your HIPAA Compliance Plan should contain a breach notification policy addressing the requirements for what notifications should be made when a cyber-incident involves patient information. Become familiar with the HIPAA breach notification process, as well as any state law notification requirements. In that regard, keep in mind that Alabama recently enacted a data breach statute that contains certain notification provisions that are more stringent than HIPAA.
6. Conduct Employee Training: Train employees on what cyber-incidents look like (e.g., provide an example of a phishing e-mail), what not to do, and who to call if an incident occurs. Research shows that unintentional employee actions account for a significant percentage of data breaches.

Taking these steps upfront before a cyber-incident occurs will help you respond to the incident when it does occur (not "if it does occur"), and, hopefully, will reduce your exposure.

Download "Cyber-Incident - Now What?" written by Kelli Carpenter Fleming.