BURR FORMAN LLP

Cyber Attacks on Health Care Entities Increasing

Articles / Publications
07.26.2022

Cyber-attacks on health care entities are becoming increasingly frequent, and the resulting data breaches are often complex. In the event of a cyber-attack, health care entities and their business associates must adhere to The Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (collectively, "HIPAA") and take the appropriate steps to respond adequately.

Step 1: Do You Have a Covered Entity?

If you have a cyber-attack with potential HIPAA implications, the first step is to determine if the attacked entity is a "covered entity" or a "business associate", as defined by HIPAA. A "covered entity" covered by HIPAA is a health care provider, health plan, or health care clearinghouse. A "business associate" of the covered entity is any individual or business that performs a service on behalf of the covered entity, and in order to perform that service, creates, receives, uses, discloses, transmits, or maintains patient information. For example, a law firm representing health care clients and obtaining patient information in the course of such representation would be a business associate.

Step 2: What Information was Breached?

Once it has been determined that an attacked entity is a "covered entity" or a "business associate", the second step is to determine what information was potentially accessed as a result of the cyber-attack. If unsecured protected health information ("PHI") was involved in the breach, the HIPAA breach notification requirements are triggered. PHI is any information that relates to the past, present, or future health condition of an individual, the provision of

RELATED PROFESSIONALS

Kelli Carpenter Fleming

RELATED CAPABILITIES

Cybersecurity & Data Privacy

Health Care

Long Term Care

health care to an individual, or the payment of health care to an individual. Because of how some health care providers handle and store patient information, an attack on a provider's system may not necessarily mean the bad actor accessed PHI. The PHI may be stored on a different server or behind stronger levels of security that were not breached. Entities must be thorough in this analysis, however, as PHI may be located in unexpected places, such as e-mails, computer hard drives, or public drives.

Step 3: Who Must be Notified?

Once it is confirmed that the attacked entity was a "covered entity" or "business associate" and that PHI was involved in the incident, the breach reporting process under HIPAA must be initiated. This process has several layers.

The first layer is reporting the incident to the patient. When looking at a widespread cyber-attack with a vast amount of information, it can take weeks to sift through the information to determine which individual's information was involved in the attack, and may even require a data review team to determine which patients must be notified.

Once patients are identified, the breached entity must send a letter within 60 days of the discovery of the incident to the individuals. This letter must include particular elements and should be provided in a certain manner. Thus, it is important to get legal counsel involved in the drafting and notification process. For example, HIPAA addresses what to do when you have a deceased patient or when you have out-of-date or insufficient contact information for an individual. In addition, the notification should include elements that show efforts of good faith to provide the patient with all the information they need in order to protect themselves from identity theft.

The next layer of the notification process is notification to the Office for Civil Rights ("OCR"), the federal entity overseeing HIPAA compliance. The notification must be given within 60 days, but the number of patients involved impacts when the 60-day period begins to run. If the breach involves less than 500 patients, the 60-day period does not start until the end of the current calendar year in which the breach occurred. If the breach involves more than 500 patients, the 60 days begins as of the date of discovery of the incident.

The third layer of notification is to the media. If the breach involves more than 500 individuals residing in a particular jurisdiction or state, the media must be notified within 60 days. This notification is to reputable media outlets in the jurisdiction, designed to reach the impacted individuals.

Step 4: How to Document Compliance and Prevent Future Attacks?

The most important element throughout the HIPAA breach response process is documentation. It is extremely important to maintain documentation of the entire event – when it happened, the timeline, the response, the investigation details, forensic and legal reports, copies of all notifications, information regarding insurance coverage, etc. Depending on the breach, OCR may open an investigation related to the incident. Sometimes the investigation is opened quickly, and other times it is delayed, depending on factors beyond the control of the attacked entity. Thus, documentation is important, not only to refresh

memories, but also to demonstrate to OCR that the breach response was appropriate and legally compliant.

In 2021, the health care industry was the largest industry impacted by cyber-attacks in terms of the number of individuals involved. All of these attacks have HIPAA implications. Health care entities should place emphasis on their security or IT efforts, possibly outsourcing it, to ensure information is as secure as possible to prevent these types of attacks. For example, every entity should have an updated risk assessment. Not only is it required by HIPAA, but it is also a good idea. Following a cyber-attack, these efforts should be re-visited and analyzed to determine if additional steps need to be taken in the future to prevent similar attacks.

Kelli Fleming is a Partner at Burr & Forman LLP practicing exclusively in the Health Care Practice Group. Kelli may be reached at (205) 458-5429 or kfleming@burr.com.