When a Vendor's Cybersecurity Problem Becomes Your Cybersecurity Problem

By Justin Joy, JD, CIPP

Several months ago, a medical practice was unable to access its cloud based EHR system early on a Friday afternoon. A support ticket was submitted to the EHR vendor requesting assistance for the problem. In the meantime, the practice activated its emergency procedures protocol and records of the patient visits for the rest of the day were kept on paper. When the office opened the following Monday morning, although the system was seemingly slow when staff initially logged on, by noon, the system appeared to be operating normally. Information from the paper records generated during the system outage was entered into the EHR system and, from all indications things seemed to be back to usual. The office manager who submitted the support ticket was curious however because, unlike support requests submitted in the past, the group had not received any response from the EHR company to the ticket that was submitted on Friday.

At the end of the week, the group received an email from its account representative attaching a letter from the CEO of the EHR company. Contained in the letter was a statement that the EHR vendor was investigating a security incident it experienced the prior week. The letter indicated that additional details would be provided after the company had concluded its investigation. A couple of weeks went by with no further mention from the EHR vendor about the incident. Approximately three weeks after the practice noticed the system problem, it received a letter from the EHR company stating that a data breach had occurred as a result of the incident and the practice's PHI was involved. The question then became who is going to provide notification of the breach to the practice's patients, the U.S. Department of Health and Human Services, and presuming the breach was a large one, the media?

With the growing reliance on an array of vendors, particularly for providing information technology services, the story above is becoming increasingly prevalent for medical practices of all sizes. According to a recent survey, organizations within the healthcare industry were the most common victim of attacks against third parties, i.e., their business associates, accounting for one third of these types of incidents last year.[1] Ransomware, and its particularly disruptive consequences, was the most common type of attack. These events can be catastrophic to the targeted vendor, with the disruptive effect significantly impacting the vendor's customers. In the increasingly common claims scenario above, the reason why the vendor did not respond to the support ticket was because, as is often the case, it was completely overwhelmed in responding to the incident. In many cases, because the immediate incident response has consumed all the vendors' capacity, the impacted vendor is, at least temporarily, unable to assist or even provide timely information to its medical practice customer. That can be a lonely and unsettling position for a healthcare organization who is completely dependent upon the vendor for the normal operation of the practice. It can also result in confusion for the medical practice in terms of what to do next.

Covered entities should be mindful of their obligations under HIPAA for notification in the event of a data breach. This includes a data breach occurring at or because of a medical practice's third-party business associate vendor.[2] Obligations for covering the cost of the

data breach are increasingly common provisions in services agreements between covered entities and business associates. Regardless of the existence or nature of any such provision in a services agreement or business associate agreement, under the HIPAA Breach Notification Rule, the covered entity is ultimately responsible for ensuring that proper notification is made whether that notification is made (and paid for) by the business associate, or whether the covered entity must do that themselves. There may be additional breach notification obligations pursuant to state law.

In the scenario above, the medical provider was prudent in contacting SVMIC about the incident, who in turn notified Tokio Marine HCC, who writes and administers cybersecurity coverage for SVMIC policyholders.[3] Tokio Marine can begin to assist policyholders navigating these challenging scenarios by resourcing the necessary legal and technical assistance. While the availability of coverage is subject to the terms, conditions, and limitations of the insurance policy based on the unique circumstances of each occurrence, it is prudent for insureds who receive notification about a security incident or data breach from a business associate vendor to promptly notify SVMIC about the incident. In the event the security incident is a data breach, significant costs and even liability may be involved. Even if the incident is determined, as a legal matter, not to be a data breach, the HIPAA covered entity medical provider is likely still required to take certain actions.[4] For a variety of legal and practical reasons, the earlier that notice is provided to SVMIC of these incidents, the better. In some cases, if notice of a potential claim is provided too late, coverage may be denied.

If you experience a potential cybersecurity incident, contact SVMIC as soon as possible by calling 800-342-2239 and asking to speak to the Claims department.

[1]. “33% of Third-Party Data Breaches in 2021 Targeted Healthcare Orgs,” securitymagazine.com, https://www.securitymagazine.com/articles/96965-33-of-third-party-data-breaches-in-2021-targeted-healthcare-orgs.

[2]. Obligations of HIPAA covered entity providers and organizations relating to their business associate vendors was the subject of a January 2022 Sentinel article.

[3]. For more information, including general information pertaining to limitations and notification obligations, about the privacy and cybersecurity aspects of coverage provided through SVMIC, please see the September 2021 Sentinel article, “Know Your Policy: Your Coverage and Responsibilities under the Cybersecurity Policy.”

[4]. Obligations of HIPAA covered entity providers and organizations pertaining to security incidents was the subject of a November 2021 Sentinel article.
