Obligations of Medical Practices in Responding to Data Security Incidents (Not Just Data Breaches)

By Justin Joy, JD, CIPP

Physician offices, hospitals, banks and even pipeline companies; nearly every day, there is a story somewhere about a data breach impacting these types of organizations. What is not as well publicized, however, are the much more frequent security incidents that impact any organization that has an information system. Some of these security incidents may meet the legal definition of a data breach, while most others, although potentially bothersome, do not rise to such a level. There are no means of measuring the number of security incidents impacting organizations, especially attempted but unsuccessful efforts, as many security incidents may go undetected. By some estimates, however, these incidents total in the thousands each day.[1]

Physician practices need to be aware of their obligations in responding to a security

incident, regardless of whether or not the event meets the definition of a breach under the HIPAA Breach Notification Rule. By definition of the HIPAA Security Rule,

- a security incident is “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.”[2]
- a breach is defined as “the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information.”[3]

From a high level, the definition of security incident encompasses the definition of a data breach. In other words, every data breach is a security incident, however, every security incident is not a data breach. Whether or not a security incident constitutes a data breach, the HIPAA Security Rule requires that covered entities identify, investigate, respond to, and document security incidents. These incidents may come in a variety of forms, including the following:

- an unauthorized attempt to gain access to systems such as email and networks
- installation of malicious software (“malware”) such as ransomware
- the loss or theft of a device containing data
- the unauthorized or unintended disclosure of information

Fundamentally, in order to respond to a security incident, the event must be able to be identified. Medical practices have an obligation to have systems in place for detecting security incidents and alerting of their occurrence. Many of these detection systems may be technical in nature, such as intrusion detection systems and antivirus software that generates an alert when it discovers certain threats. However, even the most sophisticated and up-to-date systems and software are not capable of detecting all security incidents. Each member of a covered entity’s workforce must know how to identify a security incident and know his/her individual responsibilities in acting when they discover such an incident.

As noted above, even small organizations can be the target of hundreds or even thousands of potential or attempted security incidents daily. As part of a medical practice’s policies and procedures, it should define what type of event constitutes a security incident requiring investigation and other action. Fortunately, most events, although potentially malicious in intent, are automated and not specifically directed at the organization or any specific individual. It is likely reasonable for a medical practice to conclude, as a matter of policy, and that no formal investigation or other response is required for these random, automated, and likely frequent events.[4]

In contrast, for other more targeted attempts, whether successful or not, a practice’s incident response policy will require an investigation and other actions. An example here is an employee who is locked out because of an excessive number of failed login attempts, but it was a malicious actor, not the employee, attempting to login. Again, many security incidents, such as this example, may not meet the legal definition of a data breach, but nonetheless require some level of prompt response to confirm there has not been a

breach, mitigate any harmful effects of the incident, and document the incident along with the outcome of the investigation.

It is important for medical practices to be mindful that, under the HIPAA Breach Notification Rule, a data breach is considered discovered from the day the breach was discovered by the covered entity, or the date, in exercising reasonable diligence, the breach should have been discovered. Many security incident investigations are complex and require considerable examination before a legal determination can be made as to whether a breach has occurred. Some leeway may be provided in certain circumstances when reasonable efforts have been made to investigate a security incident, but given the action covered entities are required to complete within 60 days (and in some cases, even sooner) of discovery of a breach, security incidents must be promptly investigated. Relatedly, agreements with business associates must contain a provision requiring the business associate to report breaches to the covered entity when discovered by the business associate. While the HIPAA regulations provide a default of up to 60 days for the business associate to report a breach to the covered entity, it is typically advisable that a contract with a business associate contain a much shorter period in which to report discovery of a security incident.

Developing and implementing a security incident policy and procedure is one of the best ways for a medical practice to prepare itself to take the necessary actions when it finds itself faced with a security incident. Like nearly every other policy and procedure for a medical practice, a security incident policy and procedure needs to be developed and implemented specifically for the unique operations of the practice. This often takes the form of a security incident response plan. While each incident plan document needs to be specifically developed and implemented, there are several common components that most plans need in order to be effective and comprehensive.

- The plan needs to provide the specific definition of a security incident, which should be based in substantive part—if not verbatim—on the definition found in the HIPAA Security Rule.
- The plan may also specify types of events that do not require an immediate investigation response because of their minimal or nonexistent risk.
- The plan also needs to identify the individual, who can be the HIPAA security and/or privacy officer, within the organization that workforce members should notify upon discovery of a security incident.
- Relatedly, the plan document should also identify the members, either by position (such as IT, HR, marketing/PR and legal counsel) or by name with contact information, of a team or committee of individuals who will be activated in the event a response is required. External resources, such as SVMIC, should also be included in the plan.
- Finally, requirements related to documentation should be included as well, perhaps providing sample reporting forms upon which the information to be collected about the event is to be provided.

Once the plan has been developed and implemented, it should be reviewed periodically, preferably by the members of the incident response team, with changes made as needed. Those involved in handling incident responses for an organization should be familiar with the general steps of the plan. The midst of a security incident response, which can often be chaotic and complex, is not the time to realize there are areas of the plan that are confusing and incomplete.

While it is no longer a matter of if, but when, a medical practice will experience a data breach, it is only a matter of hours, if not minutes, before a practice may experience another security incident. While most security incidents do not meet the legal definition of a data breach, some security incidents will require a prompt and diligent response. Promptly contact SVMIC if an incident is discovered and there is any question or concern about how your practice should respond. Addressing security incidents has unfortunately become a routine requirement for medical practices. Be sure that your practice is adequately prepared to fulfill its obligations regarding these events when they occur.

[1]. One of the first known efforts to quantify hacking attempts against computers connected to the internet revealed such an attempt on average every 39 seconds or 2,244 times a day. "Hackers Attack Every 39 Seconds," Security (Feb. 10, 2017), https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds.

[2]. 45 C.F.R. § 164.304.

[3]. 45 C.F.R. § 164.402.

[4]. Many of the events that fall in this random, automatic category are technical in nature, necessitating some technical knowledge for assessment as to whether an investigation should be categorically required as a matter of policy. HHS gives the example here of an automated "pinging" application to determine whether a computer is accessible at a specific IP address, which is often done for malicious surveillance efforts. U.S. Department of Health and Human Services, "What does the Security Rule require a covered entity to do to comply with the Security Incidents Procedures standard?", HIPAA FAQs for Professionals (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/faq/2002/what-does-the-security-rule-require-a-covered-entity-to-do-to-comply/index.html.