New Year, New Threats- Time to Review Your Cybersecurity Program

By Rana McSpadden, FACMPE

It is a new year, and criminals are consistently coming up with new cyber threats. Now is a perfect time for practices to review and update their cybersecurity programs. Over the last two years, we have focused on providing cyber articles and resources to assist our policyholders with cybersecurity. This article serves as an amalgamation of these resources for quick and easy access.

Security Risk Analysis

In our July 2021 article, Security Risk Analysis: Step One of an Effective Cybersecurity Program, Loretta Verbeck discusses the requirement under the HIPAA Security Rule to conduct a security risk analysis. While this has been a requirement for health providers since the original Security Rule compliance date in 2005, according to the 2016-2017 HIPAA Audits Industry Report, released in December 2020, lack of a thorough and accurate risk assessment is one of the most cited deficiencies in enforcement action taken by the U.S. Department of Health and Human Services.[1]

As with much of the Security Rule, how a covered entity conducts a risk analysis is scalable to the size and resources available to the covered entity. Complexity and technical expertise may dictate the risk analysis be outsourced to a third-party vendor that specializes in the risk analysis process. If complexity and/or technical expertise allows, an entity may choose to conduct the analysis internally. Regardless of methodology used, the entity will still need to review the final document for accuracy and completeness. To assist entities with conducting their own analysis, HHS provides guidance and tools as well as a Security Risk Assessment (SRA) Tool, which details all requirements and walks the entity through the steps of an analysis.

Security Controls

Cybercriminals do not always need to use sophisticated attacks to gain access to your systems. Lack of security hygiene allows weaknesses in systems that cybercriminals exploit to gain easy access. In his October 2021 article, Cyber Attack Prevention Strategies, Brian Johnson defines security hygiene as “basic and fundamental security practices that must be in place to properly secure your environment”.[2] Password use alone cannot thwart cybercriminals as they have many tactics to obtain passwords. Complex password requirements, such as utilizing upper case, lower case, numbers, and symbols in a password, may still lead to easily guessed passwords because users too often create passwords which are easy to remember. Cybercriminals may also purchase breached passwords through the Dark Web. With much of the population being creatures of habit, many users will reuse the same password for multiple sites. If one of those sites is compromised, cybercriminals potentially have access to every other account for which the individual has reused the same password. Cybercriminals may also employ social engineering to trick a user into disclosing their password by use of “sending a phishing email, impersonating a trusted person, company, or brand, containing a link to a very realistic, but fake, login screen. Once the victim’s password is entered on the bogus login screen, the cybercriminals are well on their way to compromising your network.”[3]

Mr. Johnson continues in his article by discussing various solutions to password security weakness. One of those tools is utilizing Multi Factor Authentication (MFA), which adds a second layer of authentication in addition to a password. MFA may be a text sent to a trusted device or through a push notification through an app. Mr. Johnson also goes on to discuss the risks of running outdated and unpatched software and recommends establishing a patch maintenance program to ensure the most recent and secure operating system is running on all computers and devices.

Data Backup

Imagine coming into your practice one morning and no longer having access to your medical records. Maybe the server crashed over the weekend, cybercriminals took over your systems through ransomware, or there was a fire or flood that destroyed the computers. Utilizing good data backups, systems could potentially be back up and running with hopefully minimal to no data loss. In his August 2021 article, Back It Up- The Importance of Proper System Backups, Brian Johnson focuses on the Security Rule's requirement that covered entities maintain the availability of electronic protected health information (e-PHI) through the use of data backups.

Mr. Johnson defines backups as "duplicate copies of the critical data that run your practice" and "are a core component of any Business Continuity plan…"[4] Entities must consider all systems that contain this critical data, not just the electronic health record (her). Lab systems, PACS for imaging, patient photos, and financial files are all data systems that should be considered for backup. In addition to deciding what to backup, entities should also consider how each piece of data should be backed up as some systems will require different solutions, and where to back up the data; media type (disk or tape) and physical location (cloud or onsite). Finally, consider how often each piece of data should be backed up. This schedule will be determined by the rate at which the data changes and how much data you are willing to lose. While a much tighter backup schedule may be required for data that changes often, or if the amount of data you are willing to lose is limited, a less restrictive schedule may be better for if your data changes less frequently or is not as critical to lose.

Educating and Testing Staff

Much like the HIPAA Privacy Rule requires workforce member training on privacy, the Security Rule requires entities to train their staff in the risks associated with cybersecurity. Rana McSpadden describes the process of creating an education program in her April 2022 article Cyber Education is More Than a Meeting. When creating an education program, entities should identify which staff members need education, how often to provide this education, what topics to include, and how to provide education.

Topics to consider including in a cyber education program include password management, risks associated with phishing, ransomware, and social engineering. Two articles, Don't Take the Bait in 2021 and Ransomware 2.0- The New Generation of Ransomware provide information entities can use in their education programs on phishing email and ransomware. Phishing emails "impersonate brands, companies, people, and processes you trust. Next, they play on emotional triggers that manipulate your social tendencies that include authority, urgency, fear, duty, and a desire to be helpful."[5] Staff should be educated on how to spot these and what to do if they receive one. In addition to providing education on phishing, entities may also choose to test their employee's ability to spot a phishing email. Many vendors offer a free trial; one such entity is KnowB4 who offers a free test to entities interested in starting a testing program.

Phishing is not just a threat through email, as we discussed in our October 2022 article Phishing by Fax: Do Not Become a Victim. Similar to phishing emails, criminals impersonate legitimate entities through other means, such as fax, mail, text, or phone calls. It is important to be suspicious of any unsolicited request for confidential information and scrutinize the request for any red flags that it may be a phishing attempt.

Ransomware is a type of malware that, once deposited into the system, can live undetected for an undetermined amount of time until cybercriminals initiate the attack to overtake the system and hold it for ransom. In recent years, ransomware attacks have evolved into not only holding the system hostage, but also exfiltrating the data and selling it on the Dark Web unless their ransom demands are met. [6]

Incident Plan and Response

Inevitably, regardless of the safeguards in place to prevent security incidents, an entity will more than likely experience some sort of incident potentially impacting its data or information system. Justin Joy outlines what a security incident is, how to respond to an incident, and how to develop an incident response policy in his November 2021 article, Obligations of Medical Practices in Responding to Data Security Incidents (Not Just Data Breaches). He defines the difference of an incident and a breach as:

- 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."[7]
- 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."[8]

While every breach is considered an incident, not every incident is considered a breach. Entities are required to have an incident response plan to address how to respond in the event a security incident takes place, whether it is considered a breach or not. Steps to consider when developing that plan include:

- 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.[9]

In Closing

There are many components to any cybersecurity program. How an entity approaches their program may help in reducing the risks of a cyber-attack. SVMIC provides many resources to assist our policyholders with developing their program as well as providing educational resources for their staff. We have recently developed a Cybersecurity Essentials resource for quick access to many of our cyber resources we have developed over the last two years. A full list of cyber resources can be found here. For access to any of our previous cyber articles, they can be found here.

If you have questions about cybersecurity or access to these resources, call 800-342-2239 or email ContactSVMIC@svmic.com.

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

Other individuals in your organization may benefit from these articles and resources, such as your administrator, privacy or security officer, or information technology professional. They can sign up for a Vantage® account here.

[1] 2016-2017 HIPAA Audits Industry Report

[2] Cyber Attack Prevention Strategies

[3] Cyber Attack Prevention Strategies

[4] Back It Up- The Importance of Proper System Backups

[5] Don’t Take the Bait in 2021

[6] Ransomware 2.0- The New Generation of Ransomware

[7] 45 C.F.R. § 164.304.

[8] 45 C.F.R. § 164.402.

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

The contents of The Sentinel are intended for educational/informational purposes only and do not constitute legal advice. Policyholders are urged to consult with their personal attorney for legal advice, as specific legal requirements may vary from state to state and/or change over time.