COSMOS
Navigate the Compliance Universe

Complete Healthcare Compliance Manual
Patient Privacy and Security: Cyberattacks

By Michelle O'Neill[1]

What Are the Effects of Cyberattacks on Patient Privacy and Security?

Cyberattacks are attacks, via the internet, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure—or destroying the integrity of the data or stealing controlled information. The individuals or organizations that carry out cyberattacks are typically called cybercriminals, and they use cyberattacks to cause damage, to create disruption, to enact revenge, for financial gain, and for purposes of cyberwarfare. Unfortunately, the healthcare sector remains the number one target for cyberattacks. This is primarily due to the value of the data that can be obtained from a successful attack and the fact that cybercriminals are aware that if they lock up systems and patient data, it significantly affects operations and ultimately patient care.

Cyberattacks are continuing to increase and cause massive chaos to the healthcare industry. In 2017, the Healthcare Industry Cybersecurity Task Force concluded that the industry was in "critical condition," and the 2017 WannaCry cyberattack is a prime example of an attack that crippled the healthcare industry.[2] The WannaCry attack infected thousands of computers throughout the world and threw the United Kingdom's National Health Service into some chaos. Although there was no evidence that patients died as a result of WannaCry, the attack still hijacked thousands of hospital computers and diagnostic equipment.[3] NotPetya was another cyberattack in 2017 and was one of the largest cybercrimes of all time. It caused $10 billion in damage to companies and affected computers around the world.[4] The company's systems were shut down for weeks and left healthcare systems unable to use their programs, including Sutter Health. Sutter Health was prepared to respond to the attack, but even with preparation, they dealt with a backlog of more than one million files that needed to be transcribed. There are times when these notes were needed urgently, and this could have been a huge patient safety issue, and from an operational perspective, how do you recover from a backlog of one million files?

Ransomware attacks and vendor-related breaches also rose in 2019. In addition, phishing campaigns tied to the Covid-19 pandemic peaked in mid-April 2020. In 2020, US federal agencies sent an alert that there was "credible information of an increased and imminent cybercrime threat" to hospitals and healthcare providers.[5] Federal agencies urged institutions to take necessary precautions to protect their networks. The agencies stated that the hackers were using a malicious software used to encrypt and lock up data. Throughout 2020, US hospitals have been targeted in a rising wave of ransomware attacks. Hospitals have been consistently hit by ransomware attacks designed designed to infect systems. As a result of these hits, healthcare providers and hospitals were strongly urged to take necessary precautions to protect their networks.

In addition to healthcare moving to the top of the list of the most expensive data breaches, cyberattacks against the healthcare industry also have the greatest impact and risk of harm to individuals. These attacks cause damage to an organization's reputation within the community that it services and threaten patient privacy, clinical outcomes, and healthcare organizations' financial resources. Losing access to patient information or having patient information held hostage greatly affects the ability of healthcare organizations to effectively care

for patients. Inappropriate access to private patient information not only violates the patient's privacy but can also open the door for cybercriminals to alter patient data, which can lead to severe effects on clinical outcomes for patients.

There are many compliance risks associated with a cyberattack of patient information. The first and most important is the fact that patient safety could be affected by an attack. If a provider and/or healthcare organization is unable to effectively treat a patient because information is altered or unavailable, this can be a serious issue for the patient and ultimately affects patient safety. In addition, a cyberattack could result in a privacy breach, which affects the patient's privacy and puts the patient at risk for identity theft and other fraudulent activity.

Also take into consideration the fact that a cyberattack could result in negative press against the organization and loss of trust among patients. A cyberattack shakes patient confidence in the organization. If patients do not feel that their information is private and secure, they will not continue to seek care at the organization. This impacts patient care and ultimately can hurt the organization financially.