COSMOS
Navigate the Compliance Universe

Compliance Today - April 2019
Ten best practices for healthcare cybersecurity

By Jeremy L. Belanger, Esq., CHC

Jeremy L. Belanger (jbelanger@chapmanlawgroup.com) is a healthcare attorney with the Troy, MI office of Chapman Law Group.

- https://www.linkedin.com/in/jeremy-belanger-bb3a10a1/

Technological advances have contributed to the increased quality of patient care and reduced costs in providing care, but they have also greatly increased the threat of cyberattacks. The Department of Health and Human Services (HHS) found that "health care has the highest cost for data breaches." Thus, pursuant to the congressional mandate contained in the Cybersecurity Act of 2015, HHS along with partner groups and cybersecurity experts has released guidance (Health Industry Cybersecurity Practices) on the best practices to address cybersecurity threats facing the healthcare industry.[1]

Recent examples of cyberattacks

In recent years, there have been numerous stories of healthcare entities facing cyberattacks. In one attack in 2016, Hollywood Presbyterian Medical Center in California suffered a ransomware attack that froze all the computers at the hospital. Patient records, schedules, and documents could not be accessed, many practitioners were required to revert to pen-and-paper documentation while the system was down, and many patients had to be transferred. The hospital was only able to regain access when it paid the ransom demanded, though there is never a guarantee that acquiescing to a malicious actor's demands will result in regaining control of a system.[2]

In another attack on Peachtree Orthopedics in Georgia, more than 500 patient profiles were stolen and put up for sale on the dark web. The data included names, addresses, Social Security numbers, and other valuable information that can assist in identity theft. Another case involving a ransomware attack at Princeton Community Hospital in West Virginia froze the hospital's electronic health record (EHR) system. Although the hospital did not pay the demanded ransom, it did have to replace its entire EHR system.[3]

Recently, it has been disclosed that an authorized party had access to a system at a Missouri rehabilitation center that lasted approximately three months and potentially exposed the data of more than 4,000 patients.[4] The breach was not identified for more than a month after it occurred.

Not all cases are brought under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). There has been a growing trend of actions not based on the Federal Trade Commission Act (FTCA), which makes unlawful "unfair or deceptive acts in or affecting commerce,"[5] or state tort law. In one such case, a clinical laboratory employee downloaded the file-sharing program LimeWire to her work computer, which had inadequate security measures. Protected health information (PHI) for the patients was exposed as a result of an unauthorized party gaining access. Although the case is still ongoing, the FTC initially found that the inadequate security measures constituted "unfair trade practices."[6] As with HIPAA, there is no private right to sue under the FTCA; however, many states have similar variations that do allow a private party to sue.[7]

The official position taken is that the practices described are meant for "informational purposes only" and are not "required by nor guarantee…compliance with federal, state, or local laws."[8] This may be the intention of HHS, under HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act and the implementing regulations, but part of the basis for determining the amount of a civil penalty assessed against an entity after a breach occurs is whether it exercised "reasonable diligence"[9] or whether the cause of the breach "was due to reasonable cause and not to willful neglect."[10] Thus, compliance with the practices in the HHS guidance will likely be highly relevant when determining whether an entity's practices were reasonable when assessing a penalty against an entity for a breach of PHI or determining whether they may have acted reasonably under state law.