LEGAL CORNER

Data Breaches: Neurosurgery Practices Must Be Proactive and Prepared

By Bruce Armon

The potential exposure for neurosurgeons and their administrative leaders—in private practice and hospital-employed and academic medical center environment—is how to respond and act when a breach of the protected health information occurs. The HIPAA Security Rule regulations defined a breach as "the acquisition, access, use or disclosure of protected health information in a manner … which compromises the security or privacy of the protected health information."

If a suspected breach were to occur, there is a four-part test that must be undertaken. It's important to note that the presumption under the Security Rule is that a breach did occur, unless the analysis demonstrates that there is a low probability that the protected health information has been compromised.

Earlier this year, IBM Security and the Ponemon Institute released their 2019 Cost of Data Breach. The report was assembled following interviews with representatives from more than 500 companies across the private and public sectors, including healthcare and many other industries, that experienced a data breach during the measured timeframe. According to the report, healthcare had the highest industry average for the cost of a data breach, at approximately $6.45 million. This amount is 65% higher than the overall average costs of a data breach. The next highest-cost industries with respect to a data breach were the financial, energy and industrial sectors.

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has enforcement jurisdiction with respect to alleged HIPAA privacy and security lapses within the healthcare sector. In 2016, there were 13 settlement agreements announced by OCR and 10 settlement agreements in each of 2017 and 2018. The financial penalties with respect to these settlements were significant: 2016 ($23.5M); 2017 ($19.4M); and $25.7M in 2018 which is the highest annual settlement amount to date. The average HIPAA settlement amount increased from $1M in 2015 to $2.6M in 2018.

Complaints, cost of addressing them, rising

The HHS received almost 26,000 health law privacy complaints in 2018, compared to just over 17,000 received in 2015, according to data published on its website. There is no private cause of action under HIPAA; all complaints are investigated by OCR through its regional offices around the country. If your practice or organization ever becomes involved in an OCR query, it can be very time consuming. And if a settlement is reached can be very costly to the organization.

> "Neurosurgeons must be aware of their state privacy laws, and also be aware of multiple state laws if they or their employer practice in multiple jurisdictions."

A recent study published from HHS entitled "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" noted that four in five physicians have experienced some form of a cybersecurity attack and that $6.2B (billion) was lost by the U.S. health care system in 2016 due to data breaches. The study identified several critical cybersecurity threats that neurosurgeons and their practices/employers should be mindful of:

- Email phishing attacks
- Ransomware attacks
- Loss or theft of equipment or data
- Insider, accidental or intentional data loss
- Attacks against connected medical devices that might affect patient safety

In addition to activity at the federal level, many states are adopting their own privacy laws. Contrary to many relationships between federal and state statutes in which federal law preempts state law, HIPAA expressly allows a state that has a "more stringent" privacy law to be permitted. In essence, HIPAA creates a floor of privacy protections that a state can exceed. Neurosurgeons must be aware of their state privacy laws, and also be aware of multiple state laws if they or their employer practice in multiple jurisdictions.

Given the changing and increasingly risky environment, what steps should a neurosurgeon, practice or hospital employer take with respect to HIPAA privacy and security issues? Following are the key ones.

- Ensure that comprehensive policies and procedures are in place and update them as needed. Inevitably, if a complaint is received by OCR, they will want copies of the organization's policies and procedures.