SpencerFane®

Trends in Health Care and the Intersection of Cybersecurity

The health care industry is the most targeted for data breaches. A combination of health information, financial information, and research and development have made health care information more valuable on the dark web than information stolen from banking and financial institutions.

Trends

The U.S. Department of Health and Human Services (HHS) requires that breaches affecting more than 500 patients be reported, and from there, it is publicly listed on a database. Since HHS has been tracking and trending these breaches in 2009, there has been a noticeable shift in the main causes of breaches. From 2009-2015, loss and theft of records dominated the breach reports. The adoption of electronic health care records jumped to almost 100% in just four years for hospitals between 2010-2014. I remember being a staff nurse in 2009 in a large, urban hospital. We used paper charting, medication administration records (MARs), and a DOS-based system (where you couldn't use a mouse) to document assessments, notes, and care plans *concurrently*. The transition to a fully electronic health record (EHR) system at my hospital was made in 2011. While it was a relief to not have missing pages stapled to the back of your paper MAR –not to mention the joys of interpreting the handwriting of rushed physicians – it has since caused other issues.

The move to digital recordkeeping and widespread use of data encryption have been key in reducing physical loss and theft but gave rise to other risk. From 2018-2022, the trend has moved to hacking and IT incidents. HHS has reported a 93% increase in large breaches, and a 278% increase in large breaches involving ransomware.

Continuing trends in health care, including remote patient care and monitoring the utilization of telehealth and smart devices, is expected to continue into 2024. The attack surface for hackers continues to expand, with the health care sector relying on EHRs, cloud services, telehealth platforms, and mobile apps. Additionally, the use of managed and hosted service providers has continued to increase. Third-party providers and cloud-based platforms are attractive to health care providers and organizations because they reduce their operational costs, improve efficiency, and provide access to specialized services and tools. Above all, it allows them to focus on core competencies, like providing care. It is this reliance on third-party providers though that cause new challenges, including ensuring the security and privacy of data, managing their contracts, and monitoring the performance and compliance of vendors. It also means that hospitals and providers are prohibited from patching issues themselves. In the meantime, care can come to a halt.

The Financial Bottom Line

Did you know that the average data breach costs $4.45 million to resolve? That's about $165 a record, and across all industries. But, for the 13th year in a row, health care breaches are the costliest and are now an average $10.93 million to resolve. That's more than twice the average. Most of the costs involve the availability and reliability of health care technologies and systems, but there are associated costs with notifying patients and fines levied by HHS. More than half of health care organizations pass the costs of breaches to consumers (i.e., patients). However, patient trust and organizational reputation may also take a hit: 80% of patients say they'd switch providers if their data was compromised, and 50% would avoid a provider that had experienced a cyberattack.

What Can the Individual Provider Do? A Case Study

The most common attacks are perpetrated through phishing. Research supports that a burned-out staff are more prone to falling for phishing attempts.

One of my provider friends relayed to me how good phishing has become. While at work, she received a phone call from the Drug Enforcement Administration, advising her that her credentials may have been compromised and to verify information. It turned out, it wasn't the DEA at all: It was a phishing attempt. We marveled about

this. They had her cell phone number, her place of business, and her NPI. They even spoofed the DEA on the caller ID. Scammers are getting more sophisticated since the advent of Nigerian Prince Scams.

Even more alarming: breaches from stolen or compromised credentials take the longest to identify and contain. On average, it takes nearly a year (328 days) to resolve.

Takeaways:

- For hospitals and organizations, review your legacy systems for ones that are more up to date and secure.
- For providers, the government or an agency will not ask for your personal information over the phone. If they're legit and calling you, they already have it.
- For providers and administrators,
    - Have your business associate agreement reviewed by an attorney knowledgeable in this space.
    - Know the average cost of the average cybersecurity breach, consider including it or buying-up your policy to help cover associated legal fees and notification reporting.

This blog was drafted by Christine Chasse, an attorney in the Spencer Fane Dallas office. For more information, visit www.spencerfane.com.