HEALTH IT SECURITY

Insight

Identifying the Challenges to Securing Patient Data

Numerous challenges to securing patient data post threats to health data security, including significant financial costs.

Xtelligent Staff

Originally Published September 10

Cybercriminals are putting more time and resources into stealing and monetizing protected health information (PHI). The healthcare industry is growing increasingly concerned with the harvesting of credentials to gain access to an organization's network to steal sensitive health information.

Let's look at some sobering research from the past year to assess the state of healthcare security.

Attacks on the rise

A survey by HIMSS earlier this year found that three-quarters of healthcare organizations experienced a significant security incident in the past 12 months.

These security incidents are expected to grow in sophistication, number, and complexity over the coming years.

The top concerns for healthcare organizations were data breaches, ransomware and credential-stealing malware. The top threat actors were phishing attackers (identified by 37.6 percent of respondents), negligent insiders (20.8 percent) and hackers (20.1 percent).

Attackers most often used email to gain access to the organization, comprising 62 percent of breaches. Other means of gaining access to an organization's network included:

- Web application attacks
- Compromised customer networks
- Weak passwords
- Misconfigured cloud servers
- Human error

The survey also found that most healthcare organizations' cybersecurity programs have room for improvement. Significant barriers exist for remediating and mitigating security incidents, including lack of people and financial resources.

Some organizations do not yet have formal insider threat management programs. Risk assessments widely vary from organization to organization, the survey found.

The healthcare industry's security wake-up call

In its most recent Data Breach Investigations Report (DBIR), Verizon found that the healthcare industry had 750 cybersecurity incidents last year and around 536 of those incidents involved data disclosure. Medical data was the target of two-thirds of data breaches in the healthcare industry while personal information made up 37 percent of breaches.

Most alarmingly, DBIR found that the healthcare industry is among the most ill-prepared when it comes to stopping insider data breaches. In fact, the healthcare industry was the only sector that had more internal actors behind data breaches than external actors.

Patients losing trust in the system

This poor state of healthcare data security has lead to anxiety among consumers about their PHI. According to a survey of more than 2,000 US adults by The Harris Poll, around half of the respondents were extremely or very concerned about the security of their PHI (e.g., diagnoses, health history, test results). The survey also found that US adults are most concerned about diagnosed medical conditions and diseases being mishandled or shared without their permission.

Around one-third of those respondents currently use an online portal to access their PHI, with those older than 34 more likely to use a portal than 18- to 34-year-olds—39 percent to 28 percent, respectively. Among those who chose not to use an online health portal, the top reasons cited were

xtelligent HEALTHCARE MEDIA

a preference for discussing their health in person and concerns about the security of accessing their health information online.

In a study released earlier this year by the Office of the National Coordinator for Health Information Technology, 25 percent of individuals who were offered access to their online medical records did not access that information because of patient privacy and security worries.

Devastating losses

The costs of healthcare data breaches are well documented. The annual study of data breach costs by the Ponemon Institute estimated that healthcare data breaches cost an average of $408 per record in 2018 (the highest of any industry) and nearly three times higher than the cross-industry average of $148 per record. The study also found that the average cost of a data breach across industries and countries is $3.86 million, a 6.4 percent increase from 2017 and a nearly 10 percent net increase over the past five years. Ponemon analyzed hundreds of cost factors surrounding a breach, from technical investigations and recovery, to notifications, legal and regulatory activities, and cost of lost business and reputation. It found that costs are heavily impacted by the amount of time spent containing a data breach, as well as investments in technologies that speed response time.

Taken together, all of this research points to deep concerns and challenges to securing patient data, not to mention the consequences for failing to do so: high emotional and financial costs. In the next article in this series, we will explore a handful of promising solutions that can help mitigate risks in the healthcare industry.