

CHARTIS TOP READS

New concerns arise for privacy and security of health data as new players enter healthcare arena

Week of July 31 - August 6, 2022

| **AUG 05, 2022**

<https://www.chartis.com/insights/new-concerns-arise-privacy-and-security-health-data-new-players-enter-healthcare-arena>

The Buzz This Week

Consumers are increasingly concerned about their health data and who can access it. A recent survey by the American Medical Association indicates that:

- More than 92% of patients believe privacy is a right and their health data should not be available for purchase
- Nearly 75% of patients are concerned about protecting the privacy of their health data

The same survey showed that patients are most comfortable with their physician having access to health data and least comfortable with social media sites, big technology companies, and employers having access. With the announcement of Amazon's acquisition of One Medical, many members of One Medical were left asking if Amazon would act in good faith with health data. Consumers remain skeptical, but Amazon has stated that it would abide by HIPAA regulations.

Meanwhile, Meta (the parent company of Facebook) and 2 California healthcare organizations are being sued for violating patient privacy, allegedly scraping health data from hundreds of hospital websites. The plaintiff alleges that Meta harvested data for use in targeted ads, while knowingly collecting patient data without authorized consent.

Access to health data has also been top of mind in the wake of the Supreme Court of the United States' decision in Dobbs v. Jackson Women's Health. Patients and legal experts are increasingly concerned about access to data related to reproductive health, including fertility tracking apps and geolocation data. In addition, data brokers continue to collect and sell datasets on millions of expecting parents.

Data security is also a priority for health systems that are often targeted by ransomware attacks. According to the U.S. Department of Health and Human Services (HHS), a recent example of a ransomware attack took place at Yuma Regional Medical Center of Arizona, disclosed in April 2022, impacted data for 700,000 individuals. In many ransomware cases, patient data is extracted and sold on the darkweb.

Healthcare data security will likely continue to be top of mind for both patients and providers. For providers and health systems responsible for protecting the health data of their patients, data security and privacy will require a shift in prioritization.

Why It Matters

These recent developments indicate that providers and healthcare systems must reprioritize their efforts toward data privacy and security. Healthcare ransomware attacks increased 328% in the second quarter of 2022. A recent report from the Ponemon Institute found that U.S. companies average \$8.19 million per breach, with attacks on small and medium-sized organizations on the rise. This includes costs associated with post-breach response and recovery, lost business, notifications, legal, and potentially regulatory fines and civil litigations. Cyberattacks and data breaches can also erode an organization's reputation, leading to an extended loss in patient revenue.

In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. We are now seeing a rate that has doubled and should expect that healthcare organizations will likely remain a target of cybersecurity threats for the foreseeable future. Healthcare data is valuable, many legacy systems exist, and the shared use of data across organizations creates vulnerabilities.

Given the increased frequency, costs, and risks associated with securing healthcare data, insurers have responded by significantly increasing premiums for coverage of cyberattacks and data breaches. Insurers are now hardening their evaluation processes by requesting more detailed information around organizations' cybersecurity programs and overall practices. Organizations that fail to produce sufficient documentation risk having higher premiums or lower coverage limits. In some cases, insurers may simply refuse to cover an organization. In response, health systems should closely evaluate the strength of their cybersecurity program and adopt a practice to navigate new cybersecurity requirements.

While many investments can and should be made to continue to enhance cybersecurity, organizations can take practical steps to thwart increased cyber threats, including: securing remote access technology and use of multi-factor authentication (MFA), ensuring remote workers secure their home environments, implementing endpoint detection and response (EDR) technologies that can detect and respond to cyber threats in real time, maintaining regular patching cycles that address new vulnerabilities, securing and testing backup and recovery capabilities, documenting and testing an incident response plan, and conducting regular workforce training.

Data privacy and security will continue to be top of mind for patients. Health systems and provider organizations should strive to maintain or improve the current level of trust that patients have with physicians that have access to health data. Re-evaluating data privacy and security prioritization within the organization

will be a critical step for providers and health systems to maintain patient trust, reduce costs, and ultimately reduce vulnerabilities associated with evolving cybersecurity threats.

RELATED LINKS

[American Medical Association](#)

[IBM Security](#)

[Becker's](#)

[Becker's](#)

[HIPAA Journal](#)

[Health IT Security](#)

Chartis Top Reads

[View All \(https://www.chartis.com/chartis-top-reads\)](https://www.chartis.com/chartis-top-reads)

Our services

[STRATEGIC TRANSFORMATION](#)

[PERFORMANCE TRANSFORMATION](#)

[DIGITAL & TECHNOLOGY TRANSFORMATION](#)

[CHARTIS CENTERS FOR AI & STRATEGIC INTELLIGENCE](#)

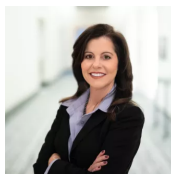
[PAYER TRANSFORMATION](#)

[STRATEGIC COMMUNICATIONS & CHANGE MANAGEMENT](#)



John Petersen

Partner



Angela Rivera

Senior Partner



Emma Bijesse

Associate Principal