Framework LTC
A SoftWriters Solution

Cybersecurity in Healthcare: By the Numbers

Did you know the healthcare industry is responsible for 70 percent of all large-scale data security incidents? In fact, nearly half of U.S. healthcare organizations have experienced a data breach over the last two years—and numbers are on the rise. That's why for all healthcare organizations, cybersecurity is more important now than ever before—and long-term care (LTC) pharmacies are no exception.

Common Healthcare Cybersecurity Threats

- Ransomware attacks
- Social engineering ("phishing") attacks
- Distributed Denial-of-Service (DDoS) attacks
- Loss or theft of equipment or data
- Business email compromise
- Accidental or intentional data loss
- Cloud security vulnerabilities
- Attacks against medical devices

Noteworthy Cyberattacks in the Past Year Alone

2023

- 8.9 million people affected — Managed Care of North America
- 11.27 million people affected — HCA Healthcare
- 8.5 million people affected — Welltok
- 13.4 million people affected — Kaiser Permanente
- 110 million people affected — Change Healthcare

2024

Repercussions of a Healthcare Cyberattack

Patient Safety Risks

- Exposed protected health information (PHI) puts patients at risk, resulting in high instances of identity theft.
- 95% of identity theft occurrences come from stolen healthcare records.
- Treatment delays caused by downtime can lead to poor health outcomes, such as longer hospital stays and complications.
- 68% of past ransomware attacks negatively impacted patient care.

Financial Losses

- Cyberattacks lead to high costs associated with ransom demands, downtime, restoration, notifications to affected individuals, and reparations.
- The average cost per U.S. data breach is $9.48 million.
- The Change Healthcare attack alone cost upwards of $2.3 billion in damages.
- The estimated cost of downtime is $14.7 billion per cyberattack.

Downtime and Delays

- Many healthcare organizations experience treatment delays due to system downtime as a result of cyberattacks.
- 71% of healthcare organizations said that ransomware impacted patient care via delays in procedures and tests.
- On average, ransomware attacks lead to 18 days of downtime.

Tips for Cybersecurity Preparedness

- **Deploy robust cybersecurity measures,** such as implementing vulnerability assessments, using multi-factor authentication (MFA), encrypting sensitive patient data, using blockchain technology, and monitoring networks for unusual activity.
- **Create an incident response plan** to secure all private data and be ready to implement data backup and recovery plans should a cyberattack occur.
- **Ensure vendors are committed to cybersecurity** to avoid cyberattacks due to third-party breaches—a leading cause of cyber incidents.
- **Collaborate with healthcare IT teams** by proactively sharing emerging cyberthreats that are impacting the healthcare industry.
- **Partner with cybersecurity professionals,** such as cybersecurity firms and cybersecurity insurance companies.
- **Keep current on cybersecurity protocols** through continuous education on emerging security trends and best practices.

As you can see, cybersecurity should be a top priority for all healthcare organizations, LTC pharmacies included—and taking the right precautions is a must. Download our full Cybersecurity Preparedness Kit to learn more about cybersecurity in healthcare.

Download Today

Framework LTC
A SoftWriters Solution