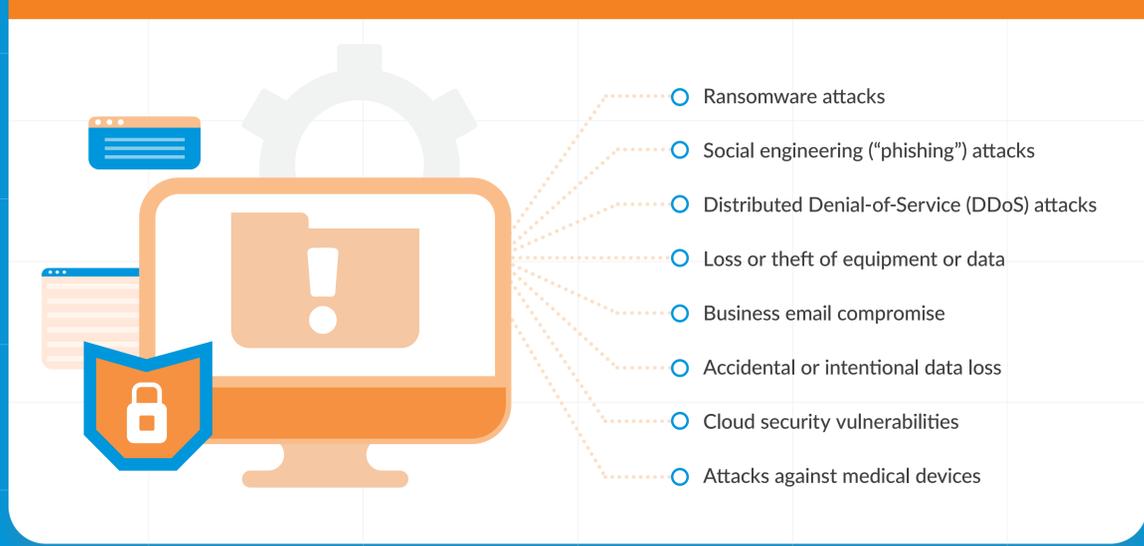


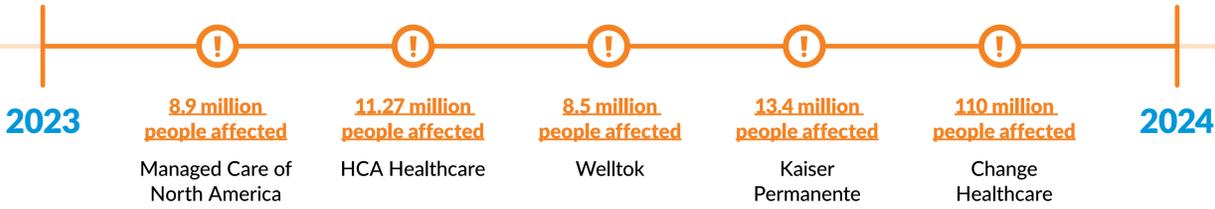
Cybersecurity in Healthcare: By the Numbers

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



Noteworthy Cyberattacks in the Past Year Alone



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 **\$948 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 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](#)