HealthManagement
Promoting Management and Leadership

# Cyberattacks' Impact on Patient Care, Safety and Trust

Cyberattacks are becoming an increasing concern within the healthcare sector. What was once considered a threat to operational efficiency has become a serious risk to patient safety and trust. Ransomware attacks, data breaches and disruptions to critical systems are affecting healthcare providers globally. These incidents are no longer just financial burdens; they undermine patient care, delay treatments and jeopardise sensitive health data. As healthcare digitises, its risks rise with broader consequences for patients and providers.

## Digitisation of Healthcare and Rising Cyber Risks

In recent years, the digitisation of healthcare has accelerated, with electronic health records (EHRs) now being widely adopted. According to recent data from the Office of the National Coordinator for Health Information Technology, over 96% of hospitals and 78% of physician offices utilise certified EHR systems. However, with this increased reliance on digital records comes heightened vulnerability. The more healthcare providers depend on electronic systems for patient care, the greater the risk of cyberattacks disrupting essential information flows.

Ransomware has emerged as a particularly dangerous threat. By holding data and systems hostage, cybercriminals place immense pressure on healthcare providers, as the inability to access vital records can delay care. In 2023 alone, the healthcare sector reported 249 ransomware attacks to the FBI, making it the most targeted industry. The attack on Ascension, a hospital system operating across 19 states in the US, is one example. Nurses reported that the inability to access digital records put patients' lives in danger, forcing them to revert to inefficient and outdated paper charting methods.

## Impact on Patient Safety and Care Delivery

The effects of cyberattacks on patient care can be far-reaching. The entire care delivery process is disrupted when hospitals and other healthcare providers lose access to digital systems. For instance, in 2023, Manchester Memorial Hospital in Connecticut was forced to divert emergency care patients to other hospitals after a cyberattack rendered their systems inoperable for over 40 days. This incident led to the cancellation of nearly half of the hospital's elective procedures and caused significant delays in processing diagnostic tests, such as X-rays and CT scans. These disruptions are not only inconvenient but can also directly impact patient outcomes, especially in emergency situations where time is of the essence.

Similarly, an attack on Lurie Children's Hospital in Chicago affected everything from prescription refills to appointment scheduling, creating significant backlogs and delaying critical care. Cyberattacks targeting hospitals and healthcare providers directly impact patients, with many experiencing delayed treatments or miscommunication between healthcare teams. The fear of further attacks erodes trust as patients doubt whether their sensitive health information and treatment will remain secure and accessible.

## Vulnerabilities in the Healthcare Supply Chain

Healthcare providers are not the only targets; their vendors and suppliers are increasingly at risk of cyberattacks. For example, the 2023 ransomware attack on Change Healthcare, a key provider of billing and data processing services, severely disrupted the operations of hospitals across the US. Change Healthcare processes payments for large payers such as Medicare and Medicaid, and its systems also manage patient claims and verify insurance coverage. Following the attack, critical operations were taken offline, severely impacting hospitals' cash flow and delaying payments.

This interconnectedness between healthcare providers and their vendors creates a broader vulnerability. When one component of the healthcare supply chain is compromised, it can have a ripple effect, causing widespread disruptions in care delivery. The attack on Change Healthcare is

considered one of the most consequential cybersecurity incidents in the history of the US healthcare system. It highlights the importance of securing the entire healthcare ecosystem, as a single breach can jeopardise the continuity of care for millions of patients.

The healthcare sector is facing an unprecedented wave of cyberattacks that threaten patient safety, trust and the stability of healthcare systems. As healthcare becomes more digitised, the risks associated with cyberattacks grow, affecting patient data and care delivery. The impact of these attacks can be devastating, delaying critical treatments, overwhelming medical staff and eroding patient confidence in the system's ability to safeguard their information.

To mitigate these risks, healthcare providers must adopt a more comprehensive approach to cybersecurity. This includes not only securing digital systems but also fostering a culture of cybersecurity awareness across all staff. By viewing cybersecurity as an extension of patient safety, healthcare organisations can take proactive measures to defend against the growing threat of cyberattacks and protect the continuity of care.

**Source: HealthData Management**

**Image Credit: iStock**

Published on : Mon, 21 Oct 2024