ATRÓMITOS
CONSULTING DONE FEARLESSLY

Cybersecurity in healthcare is critical to safeguarding sensitive patient data and ensuring the seamless operation of medical systems. This guide covers important steps to shield healthcare organizations from cyber threats and keep patients safe.

The Vital Importance of Cybersecurity in Healthcare

A COMPREHENSIVE GUIDE

“Technology is essential to healthcare, but there’s often a gap between healthcare providers and tech developers. Atrómitos fills that gap by evaluating, implementing, and securing health IT systems that meet both operational and cybersecurity needs.”

Introduction

Dear Reader,

We at Atrómitos would like to extend our heartfelt thanks for taking the time to understand the vital importance of cybersecurity in the healthcare sector.

Your commitment to recognizing and addressing these challenges is essential to safeguarding patient safety, ensuring operational continuity, and building trust in the healthcare system.

As healthcare providers and organizations face increasing threats, we must prioritize robust cybersecurity measures.

By doing so, we protect sensitive patient data and strengthen our healthcare infrastructure’s overall resilience.

We appreciate your dedication to this cause and look forward to collaborating to secure a safer future for all.

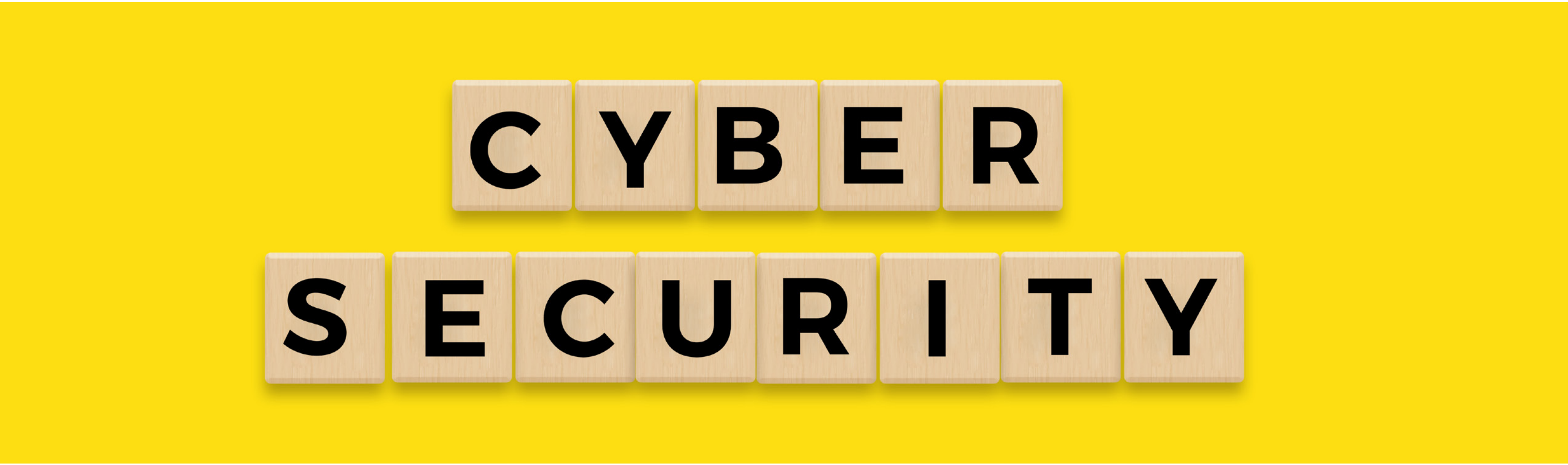
Sincerely,
The Atrómitos Team

Executive Summary

Robust cybersecurity measures in the healthcare sector keep patients and providers safe. Recent high-profile cyberattacks demonstrate that hospitals and healthcare providers are prime targets due to the sensitive nature of their data and the critical services they provide. By implementing cybersecurity strategies such as encryption, regular audits, staff training, and advanced security protocols, healthcare providers can significantly mitigate the risks of data breaches and operational disruptions.

Prioritizing cybersecurity investments and readiness is a fundamental step toward:

- **Improving Patient Safety and Trust** by protecting patient information and building trust in the healthcare system.
- **Ensuring Continuity of Care** by upgrading operational resiliency during cyberattacks.
- **Reinforcing Legal and Regulatory Compliance** by avoiding legal penalties and reputational damage.
- **Preventing Data Breaches** by reducing the risk of financial losses and legal liabilities.
- **Protecting Against Ransomware** by mitigating the impact of malicious IT intrusions.
- **Saving Money in the Long Term** by preventing costly data breaches and operational disruptions.
- **Supporting Public Health Resiliency** by safeguarding critical infrastructure and public health initiatives.
- **Strengthening Cyberattack Defenses** by collaborating with healthcare entities, cybersecurity experts, and government agencies.



Recent Healthcare Cyberattacks

In an era of digital transformation, the urgent need for adequate cybersecurity is reshaping the healthcare landscape.

The consequences of ransomware attacks in 2024 clearly show that robust cybersecurity measures are necessary to protect patient data, ensure operational continuity, and improve public trust in healthcare services.

What is a *cyberattack*?

Cyberattacks are malicious attempts to disrupt, damage, or gain unauthorized access to healthcare information technology (IT) such as computer systems, networks, or devices.

In healthcare, these attacks often:

- **Compromise** patient data, threatening confidentiality and privacy.
- **Paralyze** hospital operating systems, demanding payment to regain access and control.
- **Interrupt** medical services, delay treatments, and compromise patient safety.

Hospitals and outpatient clinics play a crucial role in providing essential medical care and face increasing cyber threats. In 2023, the United States healthcare sector set a record as a prime target for cyberattacks, with over **133 million people affected by data breaches.**

The number is rising with a record-breaking **387 cyberattacks affecting more than 45 million people** in the first half of 2024, according to a Modern Healthcare report.

The attacks led to an announcement from the Biden-Harris administration announcing plans to strengthen cybersecurity efforts for the healthcare industry.

Change Healthcare, a subsidiary of UnitedHealth Group experienced a cyberattack in February 2024. The disruption affected pharmacies, with providers unable to process prescriptions through patients' insurance, though other UnitedHealth Group systems were unaffected.

After making an unprecedented $22 million ransom payment to protect patient data, Change Healthcare discovered that **a lack of multifactor authentication (MFA)** allowed the hackers to infiltrate their systems.

In April 2024, Kaiser Permanente notified 13.4 million current and former patients about a data breach, inadvertently sharing personal information with third-party advertisers Google, Microsoft Bing, and X (Twitter).

Trackers on Kaiser Permanente's websites and mobile apps inadvertently exposed names, IP addresses, search terms, and navigation data, but not usernames, passwords, Social Security numbers, or financial information.

Ascension Hospitals were attacked in May 2024, which caused widespread disruptions including shutting down pharmacies, forcing ambulances to divert, and closing critical systems that severely impacted patient care. The shutdown led to several near-miss medication errors, and delays in processing lab results used to develop diagnoses.

Without a functioning electronic administrative system, clinicians were forced to use handwritten notes and basic computer spreadsheets to manage patient care, which increased the risk of errors and inefficiencies. Nurses and doctors had to devise makeshift solutions on the fly, leading to inconsistent and unreliable patient care tracking and coordination. These attacks are just three out of the many that have affected the healthcare industry just this year.

Impact on Patient Care

Cyberattacks can have severe consequences for patient care, as the incidents at Change Healthcare and Ascension Hospitals clearly confirm. These attacks disrupted patient care across their networks, highlighting the vulnerabilities of healthcare IT systems and underscoring the need for proper cybersecurity measures and contingency plans. Recent breaches compromised critical healthcare systems, affecting patient care in several ways:

DISRUPTING HEALTHCARE SERVICES

The ransomware attacks disrupted the processing of insurance claims and payments nationwide. At Ascension, the attack shut down pharmacies and closed critical systems. Similarly, the disruption at Change Healthcare significantly affected healthcare providers' operational efficiency, leading to billing and reimbursement delays. Such delays also strain the financial resources of healthcare facilities, potentially compromising their ability to deliver prompt, quality patient care.

JEOPARDIZING PATIENT PRIVACY & TRUST

The long-term impact of these breaches on patients can be significant, posing a severe risk to patient privacy by potentially exposing protected health information (PHI). Affected patients also may face long-term issues such as identity theft or fraud if their sensitive information is exposed. Patients expect healthcare providers to keep their sensitive information safe — any breach can erode this trust. The fear of personal data breaches can discourage patients from seeking necessary care or disclosing vital health information, ultimately impacting the efficacy of treatment plans and health outcomes.

INCREASING ADMINISTRATIVE BURDENS

Healthcare providers managed the fallout from cyberattacks by notifying affected patients, conducting internal investigations, and complying with regulations. These breaches prompted regulatory agency investigations to determine if protected health information was exposed and if healthcare providers complied with patient privacy laws. Non-compliance findings can result in more regulations and oversight, as well as fines by the Federal Trades Commission, which increase healthcare providers' operational complexity.

GROWING FINANCIAL STRAIN ON HEALTHCARE SYSTEMS

The financial costs of cyberattacks on hospitals are *substantial*, consisting of recovery expenses and regulatory fines. UnitedHealth's payment of a $22 million Bitcoin ransom and the reconstruction of Change Healthcare's compromised IT platform represent significant costs. Plus, potential regulatory fines and legal fees can further tighten healthcare provider budgets. These unexpected expenses can overwhelm healthcare organizations and lead to cutbacks in services, staff, or investments in quality improvement initiatives, ultimately affecting patient care quality.

ENHANCING CYBERSECURITY MEASURES

These attacks highlight the critical need for robust cybersecurity measures in the healthcare sector. The lack of multifactor authentication (MFA), a basic security protocol, allowed hackers to infiltrate healthcare IT systems. Strengthening cybersecurity practices, such as implementing MFA across all systems, conducting regular security audits, and training staff to accurately identify malicious phishing attempts, are essential to protect patient data and ensure uninterrupted healthcare services.

Vulnerabilities in Healthcare IT

In today's rapidly evolving digital environment, healthcare IT systems face significant and multi-faceted vulnerabilities in patient data security and the operational integrity of critical healthcare services. Such weaknesses include:

- **Legacy Systems:** Many hospitals use outdated software and hardware with security flaws or lack vendor support for updates and patches.
- **Human Error:** Staff may inadvertently expose sensitive data by clicking on phishing links or mishandling records.
- **Insider Threats:** Employees with access to patient records may misuse or improperly handle data.
- **Ransomware Attacks:** Hospitals are frequent targets due to the critical nature of patient care.
- **Internet of Things (IoT) Devices:** Increasing the use of "smart" devices expands the number of vulnerabilities a hacker can exploit.
- **Interoperability Issues:** Sharing patient data across systems makes it more susceptible to attacks if not securely managed.
- **Data Breaches:** External attackers may manipulate system weaknesses to gain unauthorized access to patient records.
- **Regulatory Compliance:** Healthcare institutions must follow regulations like the Health Insurance Portability and Accountability Act (HIPAA), which adds more complexity to security measures.

Addressing these issues is crucial to improving patient trust and safety, as well as ensuring the seamless functioning of healthcare operations.

Ensuring Patient Data Security

To safeguard hospital systems and protect sensitive patient data, the following key healthcare IT strategies address the unique challenges in mitigating cyber threats:

- **Encryption:** Encrypt data to ensure it remains unreadable without the decryption key.
- **Data Access Controls:** Implement strong controls to restrict data access to only those who need it.
- **Regular Security Audits and Penetration Testing:** Identify system deficiencies through tests before attackers can exploit them.
- **Employee Training and Awareness:** Train staff on cybersecurity best practices to reduce human error.
- **Patch Management:** Ensure software and systems are promptly updated with security patches.
- **Network Segmentation:** Limit the spread of malware by segmenting or clustering hospital networks.
- **Endpoint Security:** Deploy antivirus software, and endpoint detection and response (EDR) systems.
- **Incident Response Plan:** Develop and regularly update a plan to swiftly respond to security incidents.
- **Data Backup and Disaster Recovery:** Implement regular data backups and modernize disaster recovery plans.
- **Comply with Federal and State Regulations:** Ensure compliance with healthcare regulations like HIPAA.

Implementing these proactive efforts will contribute to a more secure and resilient healthcare environment where patient safety and data integrity are paramount.

Building Resilience Together

Collaboration among hospitals, cybersecurity experts, and government agencies is crucial for enhancing preparedness against cyber threats in healthcare. The National Cybersecurity Strategy Implementation Plan (NCSIP) underscores the importance of such cooperation, emphasizing public-private partnerships, a whole-of-society approach, and international collaboration. Shared expertise, strategic planning, threat intelligence, resource allocation, incident response coordination, policy development, and education and training are essential components of this collective effort. Together, these measures ensure a unified and robust defense against cyber threats, safeguarding critical infrastructure and improving overall cybersecurity resilience.

Robust and unified cybersecurity measures can prevent financial losses associated with cyberattacks, safeguard critical operational infrastructure, enhance the overall resiliency of healthcare IT, and ensure compliance with regulatory requirements. Health IT investments and cyberattack readiness are crucial for protecting sensitive patient information from breaches, ensuring uninterrupted patient care, and sustaining patients' trust in the healthcare system.