

Brief Commentary

Cybersecurity as a Patient Safety Imperative: A Brief Commentary for Healthcare Practice

Manish Chaudhary*

Lanier Healthcare Canada, 36-980 Adelaide Street South, London, ON N6E 1R3, Canada

*Correspondence: Manish Chaudhary, Lanier Healthcare Canada, 36-980 Adelaide Street South, London, ON N6E 1R3, Canada
, E-mail: dr_manish_a@yahoo.com, DOI: 10.1042/JN.6.1.0020

Abstract

Cybersecurity has evolved from a technical concern to a core component of patient safety in modern healthcare systems. Increasing reliance on digital infrastructure-electronic health records (EHRs), telemedicine, and connected medical devices-has expanded the attack surface for cyber threats. Disruptions caused by ransomware, data breaches, or system outages can delay clinical decision-making, compromise data integrity, and directly impact patient outcomes. This brief commentary highlights the critical relationship between cybersecurity and patient safety and outlines pragmatic, standards-aligned strategies for healthcare organizations, particularly small clinics, to mitigate risks. Anchored in frameworks such as the Health Industry Cybersecurity Practices (HICP 2023) and NIST Cybersecurity Framework (CSF 2.0), the discussion emphasizes scalable and actionable interventions to strengthen resilience while maintaining care continuity.

Keywords: Cybersecurity, Patient safety, Healthcare systems, Ransomware, NIST CSF, HICP, Clinical risk management

Received date: June 27, 2026; **Accepted date:** July 06, 2026; **Published date:** July 20, 2026

Citation: Manish Chaudhary (2026) Cybersecurity as a Patient Safety Imperative: A Brief Commentary for Healthcare Practice. JOB 6: 1

Copyright: © 2026, Manish Chaudhary. All intellectual property rights, including copyrights, trademarks rights and database rights with respect to the information, texts, images, logos, photographs and illustrations on the website and with respect to the layout and design of the website are protected by intellectual property rights and belong to Publisher or entitled third parties. The reproduction or making available in any way or form of the contents of the website without prior written consent from Publisher is not allowed.

Introduction

Digital transformation has significantly improved healthcare delivery through enhanced access to patient data, streamlined workflows, and increased connectivity. However, these advancements have also introduced substantial cybersecurity vulnerabilities. Healthcare organizations-especially small outpatient clinics-are increasingly targeted by cybercriminals due to limited resources, outdated systems, and insufficient security infrastructure.

Cyber incidents are no longer confined to financial or data privacy consequences; they directly threaten patient safety. Loss of system access during ransomware attacks, manipulation of clinical data, and delays in care during downtime can lead to diagnostic errors, medication mistakes, and treatment delays. As such, cybersecurity must be reframed as a patient safety issue rather than purely an IT concern.

Cybersecurity threat landscape in healthcare

Rising frequency and impact of cyberattacks

Healthcare remains one of the most targeted sectors for cyberattacks globally. Ransomware attacks, in particular, have escalated in frequency and sophistication, often crippling healthcare operations for extended periods. These attacks not only compromise sensitive patient information but also disrupt clinical workflows, forcing providers to revert to manual processes that increase the risk of error.

Operational disruption and clinical risk

Cyber incidents can lead to system outages that disrupt access to essential patient information such as medical history, allergies, laboratory results, and imaging. In time-sensitive clinical settings, even short disruptions can have serious consequences. Additionally, the integrity of clinical data may be compromised, raising concerns about inaccurate diagnoses or inappropriate treatments.

Medical device vulnerabilities

The growing adoption of internet-connected medical devices (IoMT) has introduced new vulnerabilities. Many devices operate on legacy systems that cannot be easily patched, making them attractive targets for cyber exploitation. Compromised devices can malfunction or provide incorrect readings, directly endangering patient safety.

Cybersecurity as a patient safety priority

The shift toward recognizing cybersecurity as a patient safety priority is supported by healthcare organizations and regulatory bodies. Cyber incidents should be treated similarly to other clinical risks, such as medication errors or hospital-acquired infections.

Safety implications

- Delayed care delivery due to system outages
- Clinical decision errors due to incomplete or altered data
- Breakdowns in communication among care teams
- Reduced situational awareness in critical care settings

By integrating cybersecurity into patient safety frameworks, healthcare leaders can better prioritize investments and align technical measures with clinical outcomes.

Standards and frameworks guiding cybersecurity practices

Health Industry Cybersecurity Practices (HICP 2023)

HICP provides a set of practical recommendations tailored to healthcare organizations, particularly small and medium-sized practices. It focuses on common threats such as ransomware, phishing, and data loss, offering structured guidance on mitigation strategies.

NIST cybersecurity framework (CSF 2.0)

The NIST CSF 2.0 expands its scope to emphasize governance and enterprise risk management. It introduces a “Govern” function that highlights leadership accountability, making it highly relevant for integrating cybersecurity into patient safety initiatives. These frameworks offer a foundation for implementing scalable, cost-effective cybersecurity measures aligned with clinical priorities.

Practical cybersecurity interventions for healthcare settings

Given resource constraints in many healthcare environments, especially small clinics, the focus should be on high-impact, feasible interventions.

- **Identity and access management**

Implementing multi-factor authentication (MFA) across critical systems significantly reduces unauthorized access risks. Strong password policies, role-based access controls, and prompt deprovisioning of inactive accounts are essential practices.

- **Patch and vulnerability management**

Maintaining an accurate inventory of IT assets and medical devices enables prioritization of vulnerabilities. Regular patching of software and systems-especially those exposed to the internet-is critical in preventing exploitation of known weaknesses.

- **Data protection and backup strategy**

Secure, encrypted, and **offline or immutable backups** are a cornerstone of resilience against ransomware. Equally important is regularly testing backup restoration to ensure operational continuity during an incident.

- **Email and endpoint security**

Phishing remains a leading attack vector in healthcare. Training staff to recognize phishing attempts, combined with advanced email filtering and endpoint protection tools, can significantly reduce risk.

- **Network segmentation**

Segregating clinical systems, administrative networks, and medical devices limits lateral movement in the event of a breach. This containment strategy reduces the scope and impact of cyber incidents.

- **Medical device security**

Maintaining an inventory of all connected medical devices-including software versions and dependencies-is essential. Where patching is not feasible, compensating controls such as network isolation should be implemented.

- **Incident response and downtime preparedness**

Healthcare organizations should develop and regularly test incident response plans. Downtime procedures-including paper-based workflows and alternative communication protocols-must be clearly defined to maintain safe patient care during system outages.

- **Vendor and third-party risk management**

Third-party vendors often have access to sensitive systems and data. Ensuring that vendors follow robust security practices-including MFA and data protection measures-is critical in minimizing supply chain risks.

- **Governance and leadership engagement**

Cybersecurity must be integrated into organizational governance structures. Leadership should monitor key performance indicators (KPIs) such as system recovery time, backup success rates, and incident response effectiveness, linking them directly to patient safety outcomes.

Discussion

The increasing frequency and severity of cyber incidents in healthcare highlight the urgent need for a paradigm shift. Treating cybersecurity as a patient safety imperative ensures that it receives the attention and resources it deserves. For small clinics, the challenge lies in balancing limited resources with growing security demands. However, incremental adoption of prioritized controls-such as MFA, regular patching, and robust backup systems-can deliver significant risk reduction.

Aligning cybersecurity efforts with established frameworks like HICP and NIST CSF 2.0 provides a structured approach that is both practical and scalable. More importantly, it bridges the gap between technical implementation and clinical impact, reinforcing the concept that cybersecurity is integral to safe patient care.

Conclusion

Cybersecurity is no longer optional in healthcare-it is fundamental to patient safety. As digital technologies continue to shape care delivery, healthcare organizations must adopt proactive, standards-aligned strategies to protect both systems and patients. By implementing practical cybersecurity measures and embedding them within clinical governance frameworks, healthcare providers can enhance resilience, reduce risk, and ensure continuity of safe, high-quality care.

Declarations

Conflict of interest

None declared

Funding

No external funding received

Ethical approval

Not applicable