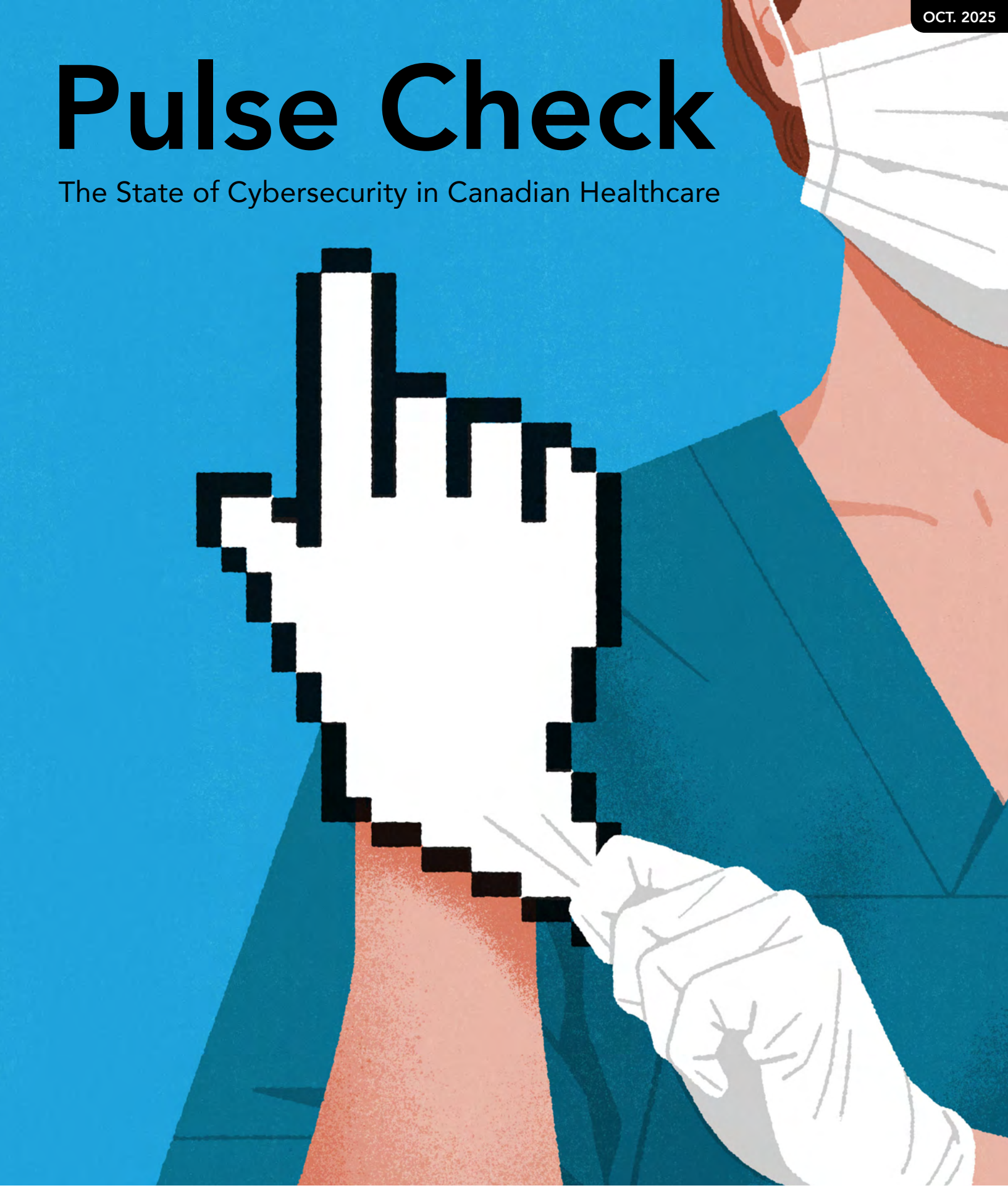
OCT. 2025

# Pulse Check

## The State of Cybersecurity in Canadian Healthcare



accerta DARKTRACE ccn

# Contents & Contributors

Matt Harrison Clough

Freelance Illustrator and the artist behind our cover.


Elias Diab

VP, Cybersecurity Advisory Services, Accerta and author of *Cybersecurity: The New Health Care Emergency in Canada.*


Dr. Benoit Desjardins

Academic radiologist and author of *Pixels under Siege: Cyber Threats to Medical Imaging.*

**Navigation Tips**

**Select** contributor head shots to view their articles and sponsor logos to visit their websites

**Yellow underlined** text indicates a link outside or within the report.


Serge Charette

Director of Solution Engineering, Tanium and author of *Securing the Front Lines of Care: Why Cyber Resilience Is Essential to Modern Healthcare in Canada.*


Ashif Samnani

Cyber Security Principal at MOBIA Technology Innovations and author of *The Great Divide: How Canada's Healthcare Cybersecurity Laws Fall Behind in a Digital World.*


Enza Alexander

Executive Vice-President at ISA Cybersecurity and author of *Five Healthcare Cybersecurity Trends to Watch in 2026.*


André Allen

Director Cyber and Technology Engagement & CISO at INQ Consulting & INQ Law and author of *Cybersecurity and Privacy in Canadian Healthcare: Navigating Critical Challenges in the Digital Age.*


Terry Cutler

CEO of Cyology Labs and author of *A Field Guide for Short-Staffed Teams: Securing Healthcare in a Digital Age.*


François Guay

Founder of the Canadian Cybersecurity Network and author of *Why Every Healthcare Worker Is Now on the Cybersecurity Frontline.*

Charlie Tsao

Engagement and Community Specialist and editor of *Pulse Check.*

Jen Spinner

Creative director of *Pulse Check.*

# Introduction

by François Guay

The Canadian Cybersecurity Network (CCN) is Canada's largest technology and cybersecurity community, uniting more than 45,000 members and 300 companies. It supports nearly a million and a half professionals, educators, and government leaders under one shared mission: to strengthen national cybersecurity by growing Canada's cyber talent, fortifying its businesses, and protecting the systems that safeguards Canadians.

## Cybersecurity Is Now a Matter of Life and Death

Healthcare has become the critical frontline in cybersecurity. Ransomware that once targeted data now directly threatens lives: delaying surgeries, shutting down hospital networks, and exposing millions of patient records. Just in the past year, attacks on Canadian healthcare systems disrupted essential services across multiple provinces.

A cybersecurity failure in healthcare is not just a technical outage; it's a public-health emergency. The digital transformation of medicine, from electronic health records to AI diagnostics and connected devices, has revolutionized care. But every advance in connectivity has expanded the attack surface. A single misconfigured system or untrained employee can mean the difference between safety and crisis.

## Canada's Healthcare Crossroads

Our healthcare infrastructure, while world-class in patient care, remains underprepared for cyber resilience. Budgets are stretched thin, regulations differ across provinces, and the cyber talent shortage persists. The Canadian Centre for Cyber Security has consistently flagged healthcare as one of the country's most targeted and vulnerable sectors. Public trust is now part of the equation. Canadians expect their health data to be treated with the same care as their health itself. Every breach erodes trust across Canada's digital health ecosystem, undermining confidence in care delivery.

This *Pulse Check* report brings together the voices of cybersecurity leaders, physicians, policymakers, and researchers to examine how Canada can move from awareness to action and from vulnerability to resilience.

**CCN Quick Tips**

**Top 5 Cybersecurity Tips for Healthcare Workers**

**1. Watch for Phishing**

Pause before clicking links or opening attachments. Verify sender addresses and report suspicious emails immediately — phishing is the #1 cause of healthcare cyber breaches.

# Executive Summary

Cybersecurity has become a frontline issue for Canadian healthcare. As digital systems underpin everything from patient records to life-saving equipment, the stakes are no longer abstract—they are clinical, operational, and deeply human. But cyber threats are intensifying and patient safety remains at risk. The *Pulse Check: The State of Cybersecurity in Canadian Healthcare* report marks a decisive moment for Canada's healthcare system. Healthcare is both the nation's most essential service and among its most vulnerable digital frontiers. This report examines the scale of the challenge, the systemic gaps that persist, and the urgent need for coordinated action across technology, policy, and culture.

## Key Findings

1. **Healthcare is the top ransomware target in Canada.** Attack frequency has surged, disrupting patient care and compromising data integrity.
2. **Human error drives most breaches.** Incidents often stem from phishing, credential misuse, or unintentional insider actions.
3. **Persistent cyber talent shortages.** Many hospitals lack dedicated cybersecurity professionals or 24/7 monitoring capability.
4. **Inconsistent cyber awareness training.** Fewer than half of surveyed organizations provide ongoing or role-specific cyber awareness programs.
5. **Interoperability gaps and legacy systems compound risk.** Outdated networks and fragmented vendor ecosystems hinder security integration.

## From Findings to Framework

Canada's healthcare cybersecurity strategy must advance beyond technology acquisition and compliance checklists. This report calls for a shift toward resilience built around people—where clinicians, administrators, and technologists are empowered to safeguard patient care. Technology alone cannot close the gaps; security depends on informed decisions, shared responsibility, and a culture that treats cyber readiness as integral to patient safety.

## CCN's Call to Action

The Canadian Cybersecurity Network urges national collaboration and investment in five key areas:

- Embed cybersecurity into every digital-health initiative—from conception to deployment.
- Invest in people, and build capacity for clinicians, administrators, and IT staff alike.
- Make cybersecurity awareness and training a national priority—centered on people and ensuring every healthcare worker understands their role in protecting patient data and systems.
- Adopt secure-by-design funding models that reward resilience, not just connectivity.
- Share threat intelligence nationally, so that every breach teaches, and no hospital stands alone.

## The Path Forward

This report is both a warning and a roadmap. The findings make it clear: healthcare cybersecurity is not merely a technical challenge; it's a matter of national health. The next phase demands decisive, coordinated action: policy reforms, funding realignments, and cultural transformation.

Cybersecurity is patient safety itself. Securing Canada's digital hospitals and clinics means safeguarding the nation's health at its core.

**CCN Quick Tips**

**Top 5 Cybersecurity Tips for Healthcare Workers**

**2. Use Strong Passwords + MFA**

Create long, unique passphrases (e.g., "three random words") and never reuse them. Turn on multi-factor authentication everywhere — it blocks over 99% of account compromise attempts.

# Cybersecurity: The New Health Care Emergency in Canada

by Elias Diab, Presented by Accerta


## Abstract

Canada's health care and social services sectors are facing an urgent cybersecurity crisis. As attacks on public systems increase, data breaches now threaten trust, safety, and the resilience of essential services, far beyond financial penalties. This article examines the unique vulnerabilities within Canada's public-sector digital infrastructure, outlines the hidden costs of breaches, and presents a secure-by-design framework to safeguard sensitive data. Drawing on Accerta's expertise, we argue that cybersecurity is now a foundational requirement for health care and social program delivery. We also explore best practices and lessons from safeguarding sensitive health data in Canadian social programs, including strategies for electronic records, mobile health apps, and secure inter-agency data exchanges.


## Introduction

In today's hyperconnected world, health care and social services depend on secure, interoperable platforms capable of handling vast volumes of sensitive data. From personal health information (PHI) and social insurance numbers to disability claims and income support records, the stakes are immense. With attacks escalating in sophistication and frequency, cybersecurity is no longer just a technical concern, it has become Canada's new health care emergency.

Nowhere is this more urgent than in programs where social services and health care converge. Protecting sensitive health data in social programs such as electronic health records requires new strategies to secure digital platforms, mobile health apps, and the complex inter-agency data exchanges that underpin modern service delivery.

# 11%

of cyberattacks in Canada last year targeted the public sector. Source: The Emerging Cybersecurity Risks Facing Canada's Public Sector, PwC Canada

## The Canadian Context: A Fragile Digital Foundation

Canada's health care and social services ecosystem is uniquely broad, complex. It is heavily reliant on social programs, such as those supporting autism, disability, dental and mental health, and low-income populations. Government agencies face a unique set of challenges: legacy systems, constrained budgets, sensitive citizen data, and overlapping vulnerabilities across departments. The dependence on digital platforms, combined with inter-jurisdictional data sharing, creates a sprawling attack surface vulnerable to disruption.

The need to protect sensitive health data in those social programs has become central to this challenge. Electronic records and mobile health apps expand access but introduce new vulnerabilities, while inter-agency data exchange multiplies the potential entry points for attackers. Best practices such as end-to-end encryption, auditing, and Zero Trust architecture must be adapted to environments where multiple service providers manage deeply personal information.

In Canada, privacy and security requirements vary by sector, but all impose strict obligations to protect personal and health information. Federally, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) set the standard for private-sector organizations, while Alberta and British Columbia operate under their own *Personal Information Protection Acts* (PIPA). In Ontario, the *Personal Health Information Protection Act* (PHIPA) governs hospitals, clinics, and other custodians of health data. Public-sector bodies in Ontario, Manitoba, and British Columbia are regulated by their respective *Freedom of Information and Protection of Privacy Acts* (FIPPA).

All these laws clearly expect organizations to implement strong security measures to safeguard sensitive data against unauthorized access, breaches, and misuse. For cybersecurity leaders, compliance is not just a legal requirement but a foundational element of trust and resilience in the digital age.

## The True Cost of a Breach

While financial impacts such as regulatory fines, lawsuits, and remediation costs make headlines, the deeper consequences are more profound and enduring. When social and health care systems are compromised, the damage is not confined to balance sheets, it undermines the lives and dignity of citizens.

- **Erosion of public trust:** A breach undermines the moral contract between governments and citizens.
- **Jeopardized safety and eligibility:** Compromised data in social and health care programs can delay disability benefits, misclassify patient needs, or disrupt eligibility determinations.
- **Operational paralysis:** Recovery involves containment, investigation, notification, and remediation, which diverts critical resources away from care and service delivery.
- **Organizational strain:** Breaches force policy changes, expensive technology upgrades, and cultural shifts, often disrupting frontline services.

## Secure by Design: A Strategic Imperative

Modernization is no longer optional; it is a strategic imperative. Agencies must adopt a secure-by-design approach that embeds protection into every layer of people, process, technology, and data. This includes addressing the realities of modern service delivery, where electronic health records, mobile apps, and inter-agency platforms form the backbone of social-health care integration.

Key elements include:

**Zero trust architecture:** Verifies every access request, regardless of origin.

**Multi-Factor Authentication (MFA):** Defends against credential theft and unauthorized access.

**Data encryption (in transit and at rest):** Protects sensitive records across their lifecycle.

**Privileged access management:** Restricts access based on roles to minimize insider threats.

**Regular risk assessments and incident response:** Ensures preparedness for emerging threats.

**Ongoing staff training:** Addresses human error, the most persistent vulnerability.

Best practices also emphasize building secure mobile health ecosystems. Encryption of app data, secure APIs for inter-agency collaboration, and mandatory security audits for third-party vendors are critical steps. Case studies from provincial ministries demonstrate how embedding audit trails into inter-agency exchanges improves transparency and accountability, reducing both technical and ethical risks.

In addition to technical safeguards, administrative and physical measures such as data-sharing agreements, continuous monitoring, and secure disposal protocols reinforce accountability and resilience.

## Embedding Cybersecurity into Modern Service Delivery

Public-sector organizations are turning to vendor-neutral advisors with deep understanding of Canada's privacy and security requirements, inter-agency data-sharing, cloud security, and citizen-facing platforms. They embed protection into procurement and program design. At the same time, they guide secure cloud adoption and modernization strategies, helping governments strengthen compliance, build public trust, and enhance the resilience of Canada's digital public sector.

## Conclusion

For Canada's health care and social services, cybersecurity is no longer optional, it is foundational. Protecting sensitive health data in social programs, from electronic health records to mobile apps and inter-agency platforms, is central to safeguarding public trust and ensuring service resilience. Protecting this information is a shared responsibility that calls for collaboration, vigilance, and innovation.

See end notes for this article's references.

Elias Diab is Vice President of Cybersecurity Consulting Services at Accerta, providing strategic guidance to public-sector leaders and organizations working across complex digital ecosystems. In this role, Elias advises on how organizations can strengthen their cybersecurity posture, integrate secure technologies into service delivery, and support the delivery of citizen-centred solutions.

Elias is a distinguished cybersecurity executive with over 25 years of leadership experience as a Chief Information Security Officer (CISO), Board Member, and Director of Security Programs across various sectors, including government, healthcare, financial services, technology, critical infrastructure, and large-scale enterprise environments.

# Trusted cybersecurity advisors: Exclusively serving the Canadian public sector.

accerta
Proudly Canadian

Accerta's Cybersecurity Advisory Services provide strategic guidance to public-sector leaders and organizations navigating complex digital ecosystems. We advise on strengthening cybersecurity, embedding secure technologies, and delivering citizen-centred solutions—exclusively for the Canadian government.

**Learn more about Accerta's Cybersecurity Advisory Services**

Certified B Corporation

Great Place To Work. Certified MAR 2025-MAR 2026 CANADA

WE ARE A LIVING WAGE EMPLOYER ONTARIOLIVINGWAGE.CA

PAIR COMMITTED
PARTNERSHIP ACCREDITATION IN INDIGENOUS RELATIONS

CANADIAN COUNCIL FOR INDIGENOUS BUSINESS

**Contact Us** www.accerta.ca governmentsolutions@accerta.ca

# Pixels under Siege: Cyber Threats to Medical Imaging

by Dr. Benoit Desjardins

## Introduction

Medical imaging has become a cornerstone of modern healthcare. It enables non-invasive high-resolution visualization of the human body at a low cost and minimal risk. It facilitates rapid diagnoses, guides therapeutic decisions, and assists in follow-up to detect complications.

The field has undergone a rapid digital transformation in the past few decades. Film has been entirely replaced by Picture Archiving and Communication Systems (PACS), which store and manage millions of digital images. Imaging has become the most interconnected and data-intensive field of modern medicine, driving the rise of teleradiology and the progressive integration of artificial intelligence (AI). Its systems are now deeply linked to Electronic Medical Records (EMR), Radiology Information Systems (RIS), the cloud, and Internet of Things (IoT)-connected devices. This has significantly improved clinical efficiency and accessibility, but at the cost of increased cybersecurity risks, including data breaches, data tampering, and ransomware attacks. Ensuring cybersecurity across complex networks is difficult. Many include legacy equipment, some always-on devices, and systems with long life cycles that are difficult to update or replace.

> A compromised imaging system can delay diagnosis, disrupt care, lead to financial losses, and jeopardize patient safety.

## Understanding the Imaging Ecosystem

Medical imaging is a complex process that spans multiple stages, from ordering and scheduling to acquisition, transmission, storage, display, post-processing, interpretation, and billing. These processes depend on a network of interconnected devices, specialized software, and formal

standards. To secure this ecosystem, one must understand the nature and function of each element to identify vulnerabilities and mitigate risks.

### 1. THE ELEMENTS OF THE ECOSYSTEM

| | |
|---|---|
| Imaging Modality | A device (e.g. X-ray unit, CT scanner) that images patients and generates imaging studies. |
| Imaging Study | A set of images from an examination, ranging from a single image (e.g. chest X-ray) to thousands (e.g. dynamic CT scan). |
| DICOM (Digital Imaging and Communications in Medicine) | The official standard for medical imaging. |
| DICOM Image | A digital file containing both an image (pixel data) and metadata (e.g. scanner model, patient name, image dimensions). |
| DICOM Viewer | Software used to display and perform basic post-processing of images. |
| PACS (Picture Archiving and Communication System) | Networked servers and workstations used to store and access medical images. |
| RIS (Radiology Information System) | A computer system for patient management, scheduling, tracking, reporting, and billing. |
| Imaging Workstation | A workstation used to display and interpret imaging studies. |
| Post-Processing Workstation | A workstation for advanced post-processing of images. |
| Imaging Server | A server that receives, stores and distributes imaging studies. |
| Imaging Archive | Long-term storage for imaging data. |

All these elements are connected by high-speed networks inside and outside hospital walls. Internally, they interface with the EMR, billing system, clinical departments, emergency rooms, labs via HL7 interface, physician offices, and patient portals. Externally, they link to data centers, the cloud, affiliated hospitals, external physician offices, remote support vendors, and AI servers. With teleradiology, they also connect via VPN to radiologists' home workstations.

Each component in this ecosystem carries unique vulnerabilities, often involving legacy hardware with outdated operating systems. Each point of failure can open the door to insider or outsider access. Without network segmentation, attackers can move laterally across interconnected devices, gaining access to sensitive data throughout the system.

Securing this ecosystem requires layered physical, technical, and administrative controls. Driven by patient mobility, research demands, and AI training, secure image sharing across institutions is a critical requirement for modern healthcare. While the American College of Radiology (ACR) advocates for the elimination of physical media (e.g. CDs/DVDs), electronic sharing introduces new obligations: access control, protection of Electronic Protected Health Information (ePHI), and end-to-end encryption.

### 2. DICOM

All medical imaging relies on the DICOM standard, developed in the 1980s by the ACR and the National Electrical Manufacturers Association (NEMA). It has evolved continually to enable interoperability among devices from different manufacturers.

A DICOM file combines image pixel data and metadata, such as patient name, scanner model, and ordering physician. This metadata contains multiple elements of ePHI, and even the pixel data may reveal sensitive patient information.

DICOM was not initially designed with cybersecurity in mind, but security features were added over time. To protect image confidentiality, media encryption (data at rest) and network TLS encryption (data in transit) were introduced. To ensure image integrity, digital signatures were added, including a Creator Digital Signature that allows an imaging device to sign an image at creation, which remains valid for its lifetime.

Encryption and digital signatures require cryptographic keys and certificates, creating significant computational and administrative burdens. As a result, many manufacturers

have not implemented these protections, and institutions fail to use them. Most medical images therefore depend on external safeguards provided by the institution, like precious gems in a museum. If these protections fail, sensitive data is exposed.

## Threat Vectors and Real-World Incidents

A single imaging study may move across multiple digital platforms, from acquisition and archiving to analysis, billing, and patient portals. Each node in this network is a potential attack point. A vulnerable PACS server, unpatched modality, or misconfigured cloud interface can serve as a launchpad for broader hospital network intrusions. Below are recent real-world incidents involving compromised imaging data.

### 1. DATA BREACHES

Medical imaging systems are rarely the primary target in cyberattacks and often protected through obscurity. Yet they are frequently compromised during broader institutional breaches. Several cybersecurity research initiatives have scanned the internet and uncovered multiple unprotected DICOM servers:

- **2017:** Massachusetts General Hospital (MGH) found 2,782 unprotected servers, 821 of them open to a DICOM connection to access images. Canada had 52 servers, 13 of which were open to a DICOM connection.
- **2018:** McAfee identified 1,100 unprotected servers, retrieved imaging data, and even reconstructed 3D body models to demonstrate the severity of the exposure.
- **2019:** Greenbone Networks discovered 2,300 unprotected DICOM servers containing 733 million medical images. Of these, 590 servers allowed direct access to 400 million images. In Canada, they found four servers containing seven million images, though individual images were not retrievable. Two months later, a follow-up scan revealed even more unprotected servers.

Although details are scarce, numerous cases of compromised DICOM servers have been documented. Many recent breaches involved independent radiology practices: Radiology Associates of Richmond, Northwest Radiologists, Pinehurst Radiology Associates, East River Medical Imaging, and University Diagnostic Medical Imaging in the Bronx. Some were forced to close temporarily, others paid millions in penalties and legal settlements.

Hospital imaging networks can be compromised both externally and internally. External attacks exploit exposed DICOM servers, while internal attackers often connect devices to poorly secured networks, bypassing perimeter defenses. In several cases, simply plugging into a hospital Ethernet port was enough to access unsecured imaging data.

### 2. DATA AND SOFTWARE TAMPERING

Breaches of medical image integrity are less common but far more dangerous than confidentiality breaches, as they can lead to misdiagnosis and inappropriate treatment. Physicians often rely on redundancy in imaging records to detect tampering and minimize patient risk.

- **2019:** In Israel, researchers infiltrated a hospital and connected a device to intercept CT images sent to PACS. Using a deep learning technique often used to generate Deepfake videos, they altered chest images in real time by adding or removing lung nodules. Nearly all local radiologists were fooled by the realism.
- **2019:** In Spain, a researcher developed a technique to embed malware in a DICOM image by replacing the 128-byte preamble with a Windows portable executable header and altering metadata. The image still behaved like a transmittable and interpretable DICOM file, yet under specific circumstances, it could execute malicious code, compromising hospital networks. Such hybrid files blur the boundaries between clinical data and malicious payloads.
- **2025:** the Philips DICOM viewer was compromised by an Advanced Persistent Threat (APT), creating a backdoor for unauthorized network access.

These incidents underscore a critical truth, imaging software is equally vulnerable as any other system, regular patches and security updates are essential.

### 3. RANSOMWARE

Ransomware has become the leading threat against medical centers. Over 60% of healthcare institutions have been involved in such attacks, some resulting in hospital closures and even patient deaths. Since imaging systems are tightly integrated with hospital networks, ransomware blocks access and jeopardizes patient care by encrypting image data. Loss of imaging access, especially in the operating room, can have a devastating impact on patient safety.

In 2020, a ransomware attack crippled imaging systems at the University of Vermont Medical Center for two weeks, forcing treatment delays and rescheduling. Radiologists had to rely on paper records and view images directly on modality consoles to make diagnoses. Similar attacks have happened at hospitals worldwide.

### 4. EMERGING THREATS

Two growing trends in medical imaging are reshaping the field: using the cloud as a central image repository and deploying artificial intelligence (AI) to improve workflow. Both introduce new vulnerabilities.

Cloud services from respected providers are usually safe and convenient, but breaches still occur. Misconfiguration of cloud storage, such as weak access controls, can expose sensitive data. Medical institutions have limited control over these risks, which largely depend on specific vendors. Fortunately, most vendors are typically giant technology firms with significantly more robust cybersecurity infrastructure than individual hospitals.

AI is revolutionizing the field of medical imaging, but it brings unique risks. Adversarial attacks can manipulate training data to mislead models, while data poisoning degrades performance. Model inversion attacks may extract sensitive patient information from trained models. Given the black-box nature and limited interpretability of most AI models, these attacks are very difficult to detect and mitigate, undermining the diagnostic reliability of the AI models.

## Recommendations

Medical imaging involves a complex combination of networks, computer systems, imaging devices and imaging data. Most of the recommendations to improve the security of such systems involve general best practices: institution security (e.g. firewalls, VPNs), network security (e.g. network intrusion detection and prevention systems, network segmentation), endpoint security (e.g. anti-malware, regular patching, least privilege access control), and proper administrative controls (e.g. cybersecurity training, incident response plans). Below are some imaging-specific recommendations.

### MEDICAL IMAGING SPECIFIC CONTROLS

The DICOM security working group (WG-14) continuously monitors vulnerabilities and recommends mitigation approaches. Although the DICOM standard includes several security features, their adoption is limited due to the complexities of key and certificate management. WG-14 promotes mechanisms that overcome these complexities, such as the Automatic Certificate Management Environment (ACME), a set of tools and standards which automates the distribution and management of keys and digital certificates.

Using ACME, manufacturers should enable default encryption for data at rest and in transit to protect image confidentiality. Imaging devices should apply Creator Digital Signature for lifetime integrity checks, and DICOM viewers should take advantage of these new digital signatures and flag potential tampering.

## Conclusion

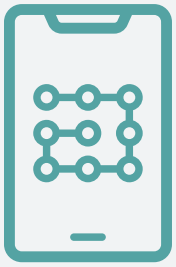
The rapid digital transformation of medical imaging has revolutionized healthcare, delivering unprecedented clinical benefits, but it has also introduced many new cybersecurity challenges, sometimes resulting in hospital closures and even patient deaths. Confidentiality, integrity, and availability of medical imaging data have been repeatedly compromised in real-world incidents, as well as in proof-of-concept attacks.

The complex and highly connected nature of imaging systems has expanded their attack surface. A multi-layered defense strategy is required to address all these challenges, combining many physical, technical, and administrative controls, as well as imaging-specific safeguards.

Dr. Benoit Desjardins, MD-PhD, is a Professor of Radiology at the University of Montreal, and an internationally recognized leader in cardiovascular imaging, artificial intelligence, and cybersecurity. He has delivered over 200 invited presentations and authored more than 100 scientific papers in these three fields. In 2024, after 35 years in the U.S., he returned to Canada as a Distinguished Professor. Dr. Desjardins is also a hacker and a member of the cybersecurity committees of HIMSS and SIIM. Outside work, he is a Black Belt in Taekwondo, a competitive marksman, and a drone racing pilot.

**CCN Quick Tips**

**Top 5 Cybersecurity Tips for Healthcare Workers**



**3. Lock and Protect Devices**
Always lock your computer or phone when stepping away. Keep software updated, use antivirus, and encrypt sensitive data — lost or stolen devices are a leading breach cause.

# Securing the Front Lines of Care: Why Cyber Resilience Is Essential to Modern Healthcare in Canada

by Serge Charette, Presented by Tanium

When a hospital's digital infrastructure goes dark, it is not just an inconvenience—it's a crisis. In 2024, one of Canada's largest health networks was crippled by ransomware: surgeries were canceled, patient data was exposed, and care teams were forced back to paper. For patients waiting for a diagnosis or a life-saving procedure, the failure of technology was a direct threat to health.

That incident is far from isolated. In June 2025, Ontario's Information and Privacy Commissioner confirmed that a ransomware attack on a shared hospital IT provider had exposed the personal health information of hundreds of thousands of patients across five institutions. The attack demonstrated the reality of modern healthcare: a breach isn't simply an IT problem, it is a disruption of care.

This is the new reality. Cybersecurity is no longer a back-office concern, it is a frontline issue with direct implications for patient safety. Every unpatched endpoint, every misconfigured cloud setting, and every overlooked medical device is more than just a technical liability, it is a potential break in the chain of care.

## The Expanding Risk Landscape

Healthcare IT leaders today face a perfect storm: constant cyber threats that disrupt care, high-stakes compliance demands, tight budget constraints, fragile legacy systems, increasingly complex distributed workforces, and aging operating systems.

At the same time, these systems sit at the intersection of two accelerating forces: the digitization of care and the escalating sophistication of cyber threats. Canada's governments are investing in electronic health records (EHRs), virtual care platforms, and integrated systems to make services more seamless and accessible. Yet every advance in connectivity creates new entry points for attackers.

The Canadian Centre for Cyber Security (CCCS) warns ransomware is no longer a question of if, but when. Its *National Cyber Threat Assessment* underscores how essential services—from hospitals and schools to municipalities—are already being disrupted. "The threat is real, the threat is growing, and we can't talk enough about it," as previously stated by Sami Khoury, Head of the CCCS.

**94%**

**of enterprises discover endpoints they didn't know existed.**

The numbers tell the same story. A 2025 global analysis of more than 2.25 million Internet-of-Medical-Things (IoMT) devices and 647,000 OT devices across 351 hospitals and healthcare delivery organizations. The study found that 89% of organizations had the top 1% riskiest IoMT devices on their networks—devices with known exploited vulnerabilities (KEVs) and insecure internet connectivity—illustrating how pervasive high-risk exposures are in healthcare environments. In Nova Scotia alone, the Auditor General reported the provincial digital health network comprises over 45,000 connected assets. Inventories and vulnerability management remain incomplete, underscoring exposure at system scale.

This isn't unique to Nova Scotia. A Vanson Bourne study found that 94% of enterprises discover endpoints they didn't know existed; in some environments, scans reveal that as many as one in five devices are unmanaged. This level of blind spot is untenable in healthcare, where every connected device represents both a patient touchpoint and a potential vulnerability,

These weaknesses are compounded by speed. Globally, well over 2,500 new vulnerabilities are disclosed each month. Traditional patching cycles, which often run for weeks or months, cannot keep pace. On average, attackers can exploit these vulnerabilities within five days of discovery, and sometimes on the very same day. Increasingly, they use AI to accelerate this effort, craft convincing phishing lures, and automate intrusions, leaving manual defenders behind.

Adding to the pressure is a chronic shortage of talent. Canada produces fewer than 4,000 cybersecurity graduates annually, while overall demand (including healthcare) is projected at 25,000. Without skilled professionals embedded in our healthcare systems, organizations are left underprepared to face industrial-scale cyberattacks. This shortfall is not just an economic gap, it is a resilience issue.

### Defense isn't Enough: Why Resilience Demands AI

Faced with this landscape, healthcare leaders must rethink their approach. For too long, cybersecurity has been defined by defense: building higher firewalls, layering on tools, and trying to keep every intruder out. While this approach remains necessary, it is no longer sufficient. Adding complexity increases costs and lowers efficiency.

Resilience must become the guiding principle. It accepts that compromise is inevitable but ensures systems, and the care they support, continue uninterrupted. In healthcare, that distinction is critical. An outage in retail may inconvenience customers; an outage in healthcare risks delayed diagnoses, canceled surgeries, and diverted ambulances.

This approach starts with visibility, a unified, continuous, real-time inventory of every device, from advanced diagnostic tools in urban hospitals to aging workstations in rural clinics. Yet many healthcare organizations operate with incomplete awareness: legacy systems, unmanaged IoT devices, and siloed data creates blind spots attackers can exploit. In a world of constantly evolving threats, the next generation of visibility is powered by lightweight endpoint agents paired with AI-driven analytics.

Acting as constant sentinels, these agents stream telemetry in real time and can trigger automated, policy-governed

actions, complementing human oversight with immediate response capabilities. When combined with AI analytics, the system moves beyond monitoring to assist decision-making: detecting anomalies, prioritizing risks by criticality and exploit likelihood, and recommending precise next steps, or even auto-remediating within defined guardrails. Together, they shift the balance of speed and precision back in favour of defenders.

Intelligent automation is the next step. With attackers moving faster than ever, manual remediation is too slow. Automated patching, anomaly detection, and compliance enforcement shrink the window of vulnerability and keep critical systems online. AI helps rank issues using live threat intelligence such as KEV and exploit probability signals, focusing effort where it matters most. Rather than predicting the future, these models surface likely hotspots and emerging patterns, so teams can act earlier, with auditability, approvals, and change control intact.

Finally, resilience requires governance. Cybersecurity cannot be confined to IT teams. CIOs, CISOs, compliance leaders, and clinical operations must align on a shared operational picture. Procurement decisions, funding models, and digital health rollouts must all embed security requirements.

This responsibility also extends beyond IT to medical devices, with Health Canada's updated guidance requiring manufacturers to consider cybersecurity throughout their operational life. Pacemakers, infusion pumps, imaging equipment, all must be secured with the same vigilance as hospital servers. These devices are no longer just clinical tools; they are endpoints in the digital health ecosystem.

### Secure by Design Embedded in Digital Transformation

Canada's health systems are modernizing rapidly. British Columbia is upgrading EHRs, while other provinces scale virtual care and remote monitoring. Federally, Bill C-72, the *Connected Care for Canadians Act*, aims to give Canadians secure, interoperable access to their health data across jurisdictions. Québec has gone even further with Law 5 (*Act respecting health and social services information*), which came into effect in July 2024, setting comprehensive standards for how health data is governed, consented, and secured–establishing a new benchmark for patient control and public trust.

But modernization without embedded security is a false promise. New EHRs, virtual care platforms, and connected systems must be secured by design through funding requirements, procurement standards, and interoperability rules from day one. This is particularly critical as AI becomes embedded in healthcare innovation. AI-powered diagnostics, predictive patient monitoring, and advanced analytics can improve care but are only as strong as the data and infrastructure behind them. Without robust security, AI can amplify vulnerabilities, creating fragile points in the very systems meant to improve patient care.

Organizations and their leaders, including health systems, should prepare now rather than wait.

Ottawa is signaling heightened expectations as the revived *Critical Cyber Systems Protection Act* (Bill C-8) imposes mandatory cybersecurity programs and incident-reporting on critical infrastructure sectors like banking, energy, and transportation. While healthcare has not yet been formally designated, the law's swift reintroduction makes clear that compliance requirements are expanding; organizations and their leaders, including health systems, should prepare now rather than wait.

### Balancing the Scales: Investing in People and Trust

Technology can only carry healthcare so far; resilience also depends on people. Every clinician, administrator, and IT staff member plays a role in protecting systems and patient data. Cybersecurity training should become as routine as infection control protocols or clinical safety drills.

Yet healthcare faces a dual shortage: clinicians and cybersecurity professionals. Hospitals will not be able to hire their way out of this gap. They must instead invest in continuous training for existing staff and plan for tomorrow's demanding workforce needs, supported by automation

that reduces manual workload and allows people to focus on patient care.

At this scale, AI and autonomous tools are essential to help bridge the gap. Emerging copilot tools and AI assistants already guide analysts through investigations, flag anomalies for deeper review, and automate repeatable tasks. In a sector where skilled professionals are scarce, these technologies act as force multipliers, augmenting human judgment rather than replacing it until the workforce can scale to meet the demand. In the long term, incentivized education and training programs must also expand their focus on cybersecurity and AI fluency, ensuring the next generation of healthcare IT professionals is equipped to thrive alongside these advancing tools.

Patients, too, are stakeholders in resilience. Trust in healthcare institutions depends as much on the protection of personal data as it does on the quality of care. A single breach undermines public confidence not just in the affected hospital but in the system as a whole.

The mandate is unambiguous: Embed resilience into every decision about digital transformation.

### The Way Forward: A Digital Health Strategy the Embeds Cyber

Canada's digital health transformation holds immense promise. Connected care can reduce inequities, expand access to underserved communities, and generate insights that improve outcomes nationwide.

When cybersecurity is embedded at the heart of what we do, healthcare organizations can confidently adopt AI-driven diagnostics, remote patient monitoring, and advanced analytics without introducing unmanaged risk. Healthcare modernization is at a critical moment for standardization, and digital transformation provides the opportunity to replace fragmented tools and legacy systems with unified, secure platforms that can scale.

Most importantly, modernization without resilience will not last. The imperative is clear, cybersecurity must be recognized as patient safety. Resilience must be built into every layer of the health system by design: in policy, in procurement, in operations, and in culture. Investments must span technology, workforce readiness, and governance.

For healthcare leaders, the mandate is unambiguous: embed resilience into every decision about digital transformation. This also means securing data before deploying AI in diagnostics, embedding agents on every endpoint to provide real-time visibility, and ensuring automation serves as a shield rather than a liability.

Patients deserve care that is safe, compassionate, and uninterrupted. Anything less is unacceptable.

See end notes for this article's references.

As Director of Solutions Engineering at Tanium, Serge Charette leads technical strategy and client engagement for some of Canada's most security-conscious, high-stakes organizations.

Every day, Serge collaborates closely with federal departments, Crown corporations and commercial enterprises to bolster their cyber resilience, enhance endpoint visibility, and expedite threat response—ensuring all solutions are aligned with business goals and regulatory requirements.

With more than two decades of leadership across cybersecurity, enterprise IT, telecommunications, satellite systems, and cloud technologies, Serge brings an extensive senior-level perspective to his current role. As a result, he has earned a reputation as a trusted advisor to senior IT and business leaders, especially in highly regulated environments where public policy, national infrastructure, and innovation converge.

A frequent speaker on topics spanning from cybersecurity agility and endpoint strategy to automation, AI, and platform consolidation, Serge has delivered key sessions at national forums including the Public Sector Network's Government Cybersecurity Showcase and the Canada IT & Security Leaders Forum.

Serge holds a degree in Computer Science and Business Administration and is fluently bilingual in both English and French.

# Stay ahead of emerging threats from critical vulnerabilities

Harness complete endpoint visibility that leads to a reduced attack surface and fewer exploit points.

**tanium.com/solutions/healthcare**

TANIUM | Canadian Healthcare

# The Great Divide: How Canada's Healthcare Cybersecurity Laws Fall Behind in a Digital World

by Ashif Samnani

## The Digital Healthcare Revolution: Promise and Peril

Canadian healthcare has rapidly digitized. Electronic health records, AI-powered diagnostics, and virtual care services now reach communities across the country. This transformation brings enormous benefits, but it also exposes the sector to significant risks. Recent ransomware attacks and data breaches have disrupted care, delayed surgeries, and revealed the vulnerability of sensitive patient information.

Healthcare data isn't like financial or administrative data. Medical histories, mental health records, and genetic information carry lasting consequences. When breached, these details can affect employment, insurance access, trusted relationships, and personal well-being for years to come. As digital adoption accelerates, the gaps in privacy and cybersecurity protections become increasingly clear.

## Canada's Patchwork Approach

Canada's approach to health data privacy begins with a federal law that sets baseline standards, but most decisions about health data governance occur at the provincial level. Each province and territory has its own framework, with varying rules for privacy, breach notification, and patient rights. This decentralized system means a person receiving care in multiple provinces may face different safeguards and obligations depending where they are treated.

Healthcare providers, in turn, must navigate inconsistent and sometimes conflicting requirements. While some regions have adopted modernized privacy laws, others maintain older practices, creating confusion, uneven protection, and challenges for organizations operating across jurisdictions. The result is a fragmented system with compliance gaps and unclear responsibilities.

## Stalled Reform at the National Level

The federal government has acknowledged these challenges and introduced legislative proposals to modernize privacy and cybersecurity standards. Bills such as C-27 and C-26 aim to establish a stronger, rights-based framework and set stricter cybersecurity requirements for critical infrastructure, including healthcare. However, progress has been slow. Delays, unclear language, and uncertainty around enforcement have slowed reforms, raising concerns that Canada may fall behind global best practices.

## Critical Weaknesses in Canadian Law

### 1. MILD ENFORCEMENT AND INSUFFICIENT PENALTIES

Canadian privacy laws rarely impose severe administrative or financial penalties for breaches. Even the largest fines are modest compared to those in other jurisdictions. This creates limited consequences for organizations that fail to invest in robust cybersecurity measures. Rather than deterrence, most enforcement focuses on corrective action, leaving little incentive to go beyond the bare minimum.

By comparison, organizations under stronger regimes often face multimillion-dollar penalties, frequent compliance audits, and strict remediation requirements. These mechanisms ensure that cybersecurity is treated as a business priority, not a procedural afterthought.

### 2. AMBIGUOUS BREACH NOTIFICATION REQUIREMENTS

Canadian law typically requires organizations to notify patients of breaches "as soon as feasible" or "at the first reasonable opportunity." While this allows for flexibility, it creates uncertainty and delays when incidents occur. Some organizations interpret these terms as days, others as weeks, and some may stretch the process for months as internal investigations unfold.

The lack of clarity and urgency can put patients at risk. When individuals are not promptly informed, they are unable to take steps to protect themselves from fraud, identity theft, or targeted attacks based on their stolen information.

### 3. UNDEFINED TECHNICAL SAFEGUARDS

Legal requirements for security remain mostly qualitative. Organizations are directed to take "reasonable precautions" or implement "appropriate safeguards," but legislation rarely defines what these mean in practice. As a result, the precise requirements for encryption, access controls, audit trails, and system updates are left up to interpretation.

This contrasts sharply with international frameworks such as General Data Protection Regulation (GDPR), which list specific technical and administrative controls that must be in place. Clear requirements encourage proactive investment and provide baselines for audits and enforcement.

### 4. LIMITED PATIENT CONTROL OVER DATA

Canadian patients generally enjoy only modest rights over their health information. Outside a few regions with progressive privacy frameworks, it is difficult to obtain, transfer, or request deletion of personal health data. The rapid growth of wearable devices, health apps, and AI-driven platforms has only widened this gap. Many consumers remain unaware of how their data is used, who may access it, or what recourse they have if something goes wrong.

Other countries guarantee broad rights of access, rectification, portability, and erasure, placing individuals at the center of decision-making about their medical information.

### 5. GAPS IN OVERSIGHT FOR DIGITAL HEALTH TECHNOLOGIES

While traditional caregivers and health institutions are generally covered by privacy laws, many digital health solutions, such as consumer apps, fitness trackers, or genetic testing services, fall outside direct regulatory oversight. These platforms amass extensive and sensitive data but are often governed only by general consumer protection or corporate privacy policies, if at all.

Without sector-specific rules, users are left to navigate complex terms of service or privacy choices, rarely grasping the full implications of sharing their data.

## International Comparisons

### UNITED STATES: THE HIPAA MODEL

The United States enforces a sector-specific regime in the form of detailed legislation applying to hospitals, health plans, and associated partners. The law imposes strict requirements for privacy officers, access controls, routine risk assessments, auditable logging, and prescribed protocols for breach notification. Enforcement can be aggressive, with large fines and the possibility of criminal prosecution for willful non-compliance.

The approach, however, excludes many consumer-facing innovations, as the rules apply primarily to traditional providers and their direct partners. This leaves gaps for health technologies that do not fit classic categories.

### EUROPEAN UNION: COMPREHENSIVE COVERAGE

Europe's legislative framework is sweeping in both scope and enforcement. Rules apply to almost any organization handling health data, from clinics to research laboratories and software vendors. Patients have extensive rights, such as accessing, correcting, and deleting data. Technical requirements are highly prescriptive, with mandatory encryption, privacy-by-design obligations, and frequent audits.

Penalties for non-compliance are significant, reaching into the tens of millions of euros or a percentage of global annual revenues. Breaches must be reported quickly, and regulators hold broad investigative powers. The result is strong protection for individuals and a harmonized regulatory environment for organizations.

Comparison Table

| Feature | Canada | USA | European Union |
|---|---|---|---|
| Notification Speed | Flexible | 60 days | 72 hours |
| Penalties | Low | High | Very High |
| Patient Rights | Limited | Moderate | Broad |
| Tech Guidance | Vague | Specific | Detailed |
| Enforcement | Infrequent | Active | Aggressive |
| Scope | Fragmented | Sector-Focused | Universal |

## The Path Forward: Reform Priorities

Comprehensive reform is needed for Canada to modernize its approach to healthcare data protection. The following steps could provide meaningful improvements:

### FEDERAL LEADERSHIP AND MODERN LEGISLATION

- Pass and enforce robust laws focused on patient rights: access, correction, portability, and erasure.
- Establish clear, detailed requirements for technical safeguards.
- Institute penalties with real deterrence value, including minimum and revenue-based fines for non-compliance.
- Recognize the extreme sensitivity of health data and include provisions tailored to medical information.

### RIGOROUS BREACH NOTIFICATION

- Mandate specific deadlines for regulators and patients—72 hours for authorities, 30 days for affected individuals.
- Ensure notifications provide clear, actionable information. Require public disclosure for significant events.

### CROSS-JURISDICTIONAL CONSISTENCY

- Set national standards so patient protections are consistent across all provinces and territories.
- Harmonize technical and operational expectations for cybersecurity, data management, and patient rights.
- Develop unified processes for appointing, training, and certifying privacy officers.

### OPERATIONAL AND TECHNICAL REQUIREMENTS

- Define minimum standards for encryption, authentication, regular vulnerability testing, incident response planning, and vendor risk management.
- Require ongoing training and awareness programs for all staff.
- Mandate comprehensive logging and regular independent security assessments.

### EMPOWERING PATIENTS

- Guarantee patients the right to see, export, and correct all health-related data.
- Enable easy-to-understand consent mechanisms modeled on best practices.
- Provide direct recourse for privacy violations, including the right to damages or corrective action.
- Educate the public about changing laws and personal responsibilities in managing digital health.

**Case Study: The Human Impact of Weakness**

A major breach at a vendor for Ontario's Health at Home system underscores the real-world consequences of regulatory shortcomings. Cyber attackers accessed records of more than 200,000 home-care patients, exposing names, diagnoses, treatment plans, and addresses for months.

Notification to affected patients was delayed for more than three months, leaving individuals unable to monitor their credit or guard against identity theft. When notice finally arrived, details were vague and support minimal. No significant penalties or public accountability measures followed, and technical remediation was understated.

If the same event had occurred elsewhere, robust legal frameworks would have triggered immediate investigation, stiff penalties, and public disclosure requirements. Patients would have had stronger legal recourse and the assurance of prompt action.

### MODERNIZING OVERSIGHT FOR DIGITAL HEALTH

- Create clear, consistent regulations for consumer health apps, wearables, and similar technologies, including certification and privacy standards.
- Define rules for emerging technologies such as AI algorithms used in diagnosis or care management.
- Establish strict controls over cross-border data flows associated with international collaboration.

### INTERNATIONAL COLLABORATION AND INNOVATION

- Maintain compatibility with major trading partners and research collaborators.
- Encourage adoption of global standards and best practices by Canadian developers and providers.
- Support Canadian technological innovation while upholding the highest privacy standards.

### IMPLEMENTING CHANGE: A PHASED APPROACH

A pragmatic implementation plan should be delivered in three phases:

- **Phase 1:** Introduce emergency measures to improve breach notification protocols and establish higher minimum penalties. Mandate immediate reporting of significant incidents.
- **Phase 2**: Broaden the legal framework to include full patient rights, specify security standards, and require consistent practices nationwide.
- **Phase 3:** Address emerging technologies, develop advanced interoperability standards, and advocate for Canada's leadership position in global health cybersecurity.

Stakeholder involvement from every sector: providers, patients, vendors, regulators, and international partners—is essential. Training, clear communication, and adequate transition time can help overcome resistance and ensure smooth adoption.

## Conclusion

Canada's healthcare system is racing toward a digital future, but its defenses remain stuck in the past. Fragmented regulation, lenient enforcement, and vague standards leave patients and institutions exposed. While some regions have taken steps forward, overall progress is slow, and the sector remains vulnerable to serious harm.

Lessons from major breaches demonstrate that reform is not just a legal or technical issue but a matter of public trust and safety. International models offer proven solutions that balance innovation with protection.

Realizing a secure, innovative, and patient-centered healthcare system requires bold legislative action, unified national standards, strong enforcement, and widespread education. As digital transformation accelerates, the risks of inaction far exceed the costs of decisive reform. Canada must seize the opportunity to lead in protecting health information for all its citizens, before the next crisis hits.

Ashif Samnani is the author of *The Great Divide* and a distinguished cybersecurity leader with extensive experience in operations, risk management, and technology security. At MOBIA Technology Innovations, he serves as Cyber Security Principal and National Practice Leader, where he drives strategic initiatives, leads managed and professional security services, and contributes to thought leadership and customer solution.

Hussain Virani is the reviewer of *The Great Divide* and is the Response Command Lead at the industrial cybersecurity company Dragos, Inc. where he actively defends assets OT/ICS environments. Hussain has over 23 years in technology, spanning across digital privacy, forensics, network communications, law enforcement, and incident response in both the IT and OT spaces.

DATA & MORE

# Our search for a unicorn

Companies that:

- Know their data → 0 Zero
- Classify their data → 0 Zero
- Have data quality for AI/LLM → 0 Zero
- Really protect their data → 0 Zero

"**Data & More** helps organizations to completely **identify**, accurately **classify** and effectively **manage** your most important data assets. "

## Deliverables

- Free assessment
- Gain valuable insights+
- Budget & Justify '26 IT projects
- Make data driven decisions
- Enable your teams
- Drive AI (successfully)
- Justify '26 IT projects & more

## Basic questions

- Is your data in the right place?
- Who has access to this data?
- Is your data compliant?
- Is your data AI ready?
- Is your security tool aware?
- What do you do with a data breach?
- What is your risk profile?

Book a 30-minute chat today and unleash your potential in every way

www.dataandmore.ca

# Five Healthcare Cybersecurity Trends to Watch in 2026

by Enza Alexander

I never imagined 2025 would be the year that my local hospital would save my child's life. When the emergency struck, it became the most important place in the world. And I know I'm not alone in my experience.

Healthcare touches many of us daily, and Canadians deserve to know that the care we rely on will be there when we need it most. Protecting our hospitals and clinical systems from cyber attacks has never been more important — and more challenging.

And, as innovation drives medical breakthroughs, it also introduces new vulnerabilities. Across Canada, hospitals, clinics, and research centres depend on a tightly connected fabric of electronic health records, diagnostic platforms, medical devices, and even "smart building" systems that keep the lights on and air clean. That connectivity powers quality care and efficiency, but it also creates real cyber risk.

When those systems fail, the consequences are immediate and serious: delayed surgeries, redirected ambulances, and scrambling clinical teams. Cyber incidents in healthcare aren't abstract, they can put lives in danger.

I have witnessed firsthand the disruption caused by "code gray" alerts as a result of cyber incidents. That's why I'd like to share an outlook for 2026: the trends most likely to shape how we defend and protect Canada's critical healthcare services.

## 1. Internet of Health Things (IoHT) & Clinical OT/IT Convergence

Canada's care environments blend medical devices (infusion pumps, monitors, imaging suites) with building and life-safety systems (HVAC, elevators, access control). Many of these assets were never designed for always-on networks, and patching them can be risky, if available at all. Over time, hospitals accumulate a mixed fleet of devices and systems that can be hard to see, segment, and update. Cyber risks don't stay confined to one system, a single compromise can cascade from business IT into clinical operations.

*Every connected device is part of patient safety: you've got to know what you have and how it's protected.*

**WHAT "SECURE" LOOKS LIKE IN 2026:**

- **Asset inventory:** I encourage our clients to build and continuously maintain a detailed asset inventory of all connected devices, including traditional IT gear as well as IoHT devices. After all, you can't protect what you can't see.
- **Network segmentation:** Segment networks to isolate IoHT devices, limit access, and contain spread in case of a successful cyber attack. Look to isolate life-critical equipment to mitigate risk.
- **Zero-trust architecture:** Tighten access to resources using a least-privilege approach reinforced by strong MFA. Look to begin a zero-trust journey if it hasn't started already.
- **Vendor management:** In procurement, demand supplier transparency. Examples include: patch SLAs, secure update practices, software bills of materials where feasible, and keeping fleets current.

## 2. LLM & AI Security (Guardrails for PHI and Model Integrity)

Generative AI and large language models are entering triage support, documentation, and patient engagement environments. Without guardrails, patient health information (PHI) can leak into prompts, logs, or third-party tools. At the back end, prompts, retrieval indexes, or decision-support data sets need to be secured. Tampering can lead to inaccurate or malicious responses, with potentially disastrous consequences. The rapid rise of AI has caught many organizations flat-footed, governance has lagged behind technology, and the gap is widening. I have never seen such a dramatic shift.

*Better, faster workflows are always welcome: as long as they're private by design and secure by default.*

**WHAT "SECURE" LOOKS LIKE IN 2026:**

- **Use only approved AI tools and channels:** Recognize that people are going to be using AI. Use data loss prevention (DLP) techniques to keep your data secure. Put DLP/PHI redaction at chat and API boundaries to prevent accidental disclosure. This keeps your patient information inside your walls, and under your rules.
- **Watch for unapproved tools:** Be on the lookout for what I like to call "shadow AI". Block unknown browser add-ons and pop-up chatbots that may quietly send data outside the organization.
- **DLP by default:** Strip out patient identifiers by default – remove sensitive PHI like names, numbers, and dates of birth to prevent accidental disclosure.
- **Keep AI chats "forgetful":** where possible, set tools to retain as little as possible, for as short as possible, so sensitive details don't linger.
- **Lock the AI's reference library:** Only trusted, current, and approved medical content goes in. Changes require sign-off so no one can poison your large language models with inaccurate content, maliciously or otherwise, with inaccurate content.
- **Test before touching care:** Pilot new healthcare uses for AI in a safe "sandbox" environment, and clearly document approvals so your teams know what's cleared and what isn't. Agentic AI has the power to improve efficiency and accuracy, when used correctly.
- **Security awareness training:** Make sure your cyber training includes modules on AI. Publish a one-page guide that features plain language examples and ideas (e.g., "Don't paste lab results into public chatbots"). Make the rules practical and easy to follow – and be sure to test staff knowledge regularly.
- **Name a single owner for AI safety:** Assign one accountable leader. This ensures your team knows exactly who to contact for questions or concerns, keeping decisions fast, consistent, and well documented.

## 3. Ransomware That Disrupts Care

Ransomware operators understand the leverage of downtime in healthcare settings. Their aim is not limited to data theft; it is the operational paralysis that pressures victims into paying a ransom. The Canadian Centre for Cyber

Security (CCCS) highlights that ransomware incidents in healthcare have been "steadily increasing worldwide" and, by one estimate, "have nearly doubled since 2022." The impact is twofold: clinical disruption, measured in delayed care and heightened patient safety risks, and financial damage, measured in ransom payments and prolonged recovery efforts. And the costs are staggering: according to IBM's *Cost of a Data Breach Report 2025*, breach costs in healthcare now average USD $7.42M, the highest of any sector studied.

*Cyber attacks are inevitable. If you plan for the worst today, you'll be ready for tomorrow.*

**WHAT "SECURE" LOOKS LIKE IN 2026:**

- **Keep immutable, offline-recoverable backups:** Increasingly, the bad guys target backups as well as live data. Keeping these snapshots isolated and protected will give you a fallback position in case of a ransomware attack. And test those backups regularly! How long do they take to restore? Do they even work?
- **Enforce multi-factor authentication (MFA) everywhere; retire legacy protocols:** Make sure that all resource access is insulated with MFA. Even now, some staff use MFA while administrators bypass it through back doors—this practice must end.
- **Pre-authorize containment actions:** Incident response (IR) testing increasingly includes clear 'pull-the-plug' scenarios to let responders isolate network segments without delay. This way, if a system or service is compromised, quick isolation limits the spread of ransomware and contains the blast radius.
- **Run clinical downtime tabletop exercises:** Rehearse paper orders, lab/radiology contingencies, and diversion communications with clinicians. It's critical to build muscle memory in advance so you can respond confidently. Tabletop exercises and IR playbooks are critical. They can help keep people alive during a crisis.
- **24/7 detect-and-respond:** AI-powered EDR and XDR solutions support rapid triage and response to cut dwell time when minutes matter. The bad guys often strike after hours and over long weekends when technical resources aren't typically at full complement.

### 4. Third-Party & Supply-Chain Exposure (Vendors, Diagnostics, Cloud, Building Services)

Canadian hospitals rely on an intricate mesh of external partners: labs and imaging portals, transcription services, scheduling and billing systems, remote service channels for devices, and even the software that runs elevators and access control. A weakness in any link can cascade through healthcare systems and affect patient outcomes. Recent Canadian disruptions caused by a shared IT provider show how quickly outages can spread.

*Your security posture extends to every partner login – treat vendor access like it's your own.*

**WHAT "SECURE" LOOKS LIKE IN 2026:**

- **Tier third parties by PHI volume and clinical criticality:** Healthcare facilities can have hundreds of suppliers and partners. To manage risk efficiently, map data flows to identify where a breach could cause the most harm.
- **Contract for security outcomes:** Negotiate breach SLAs and DPAs; require sub-processor transparency; mandate coordinated disclosure and secure update clauses; and perform risk assessments on all third parties.
- **Require signed, secure updates:** Despite best efforts, third-party software or systems can be compromised. Make sure that every update or patch for your system is signed and verified, so only authentic, safe software runs on your devices. Maintain tested rollback plans to minimize supply-chain risks to clinical and building systems.
- **Grant vendor access on a "need-to-know" basis:** Give outside companies access only the systems they need to touch, for a limited time, and record what they do. That's "zero trust" in practice: don't trust by default; always verify. And never share credentials across multiple vendors or providers – how can you track activities if you don't know who's who?
- **What can the Internet see about your organization?:** Open internet scans as well as dark web monitoring can give you an early warning that you may have suffered a compromise. Set up alerts for new servers, logins, or pages tied to your domain so you can act before attackers do.
- **Include partners in your tabletop exercises:** Don't just focus on your internal staff when conducting tests. Run downtime drills that include your shared IT service providers, vendors, and other third parties as appropriate. Agree on roles, contacts, and hand-offs so there are no gaps when a real incident hits.

### 5. Converged Physical + Cyber Safety (Access Control, Video, Life Safety)

Badge systems, infant protection systems, nurse-call systems, surveillance cameras, and elevators are part of the hospital's safety infrastructure, and they're all digital. The same intelligence that enhances safety can also create new attack paths if unmanaged. Lessons from operational technology (OT) security apply directly to healthcare: protecting people means protecting the systems that protect them. AI-enabled surveillance and analytics promise faster response, but they also require governance to address privacy, bias, and misuse.

*We need to treat healthcare facilities as a single engineered system: protect the data, controls, and the physical space with the same rigour you'd expect of clinical care.*

**WHAT "SECURE" LOOKS LIKE IN 2026:**

- **Govern as one team:** Align corporate security, facilities, bio-med, privacy, and IT under one risk register and playbook. Too often, physical security operates in isolation from IT, creating blind spots attackers exploit.
- **Isolate physical-security networks:** Segment badge readers, cameras, and door controllers on their own network; remove default passwords; avoid "flat", single-layer networks; give people only the access they truly need; and restrict system-to-system communication.
- **Balance safety with privacy:** Define clear rules for what video and access logs you keep and for how long, and ensure AI-enabled analytics comply with Canadian privacy law and hospital policy.
- **Test "converged failure" scenarios:** Simulate combined physical and IT outages—doors that won't unlock, elevators that stop, infant-protection alarms—to clarify roles, communication, and hand-offs under pressure.
- **Harden vendor remote access:** When outside technicians connect to life-safety systems: require strong sign-in, limit access to the specific system they're fixing, and record their sessions so you can review any changes.

## Bringing It All Together for Canadians

Canada's healthcare threat picture is clear, but so is our path forward. Heading into 2026, boards and executive teams should set clear accountability with their C-suite, and stand up a clinical cyber council that unites bio-med, facilities, privacy, and corporate security. Make IoHT visibility and network segmentation a first-line priority to identify connected assets and isolate systems that keep patients safe. Put incident recovery on a stopwatch: prove you can restore within clinical time limits and pre-authorize isolation actions. Run AI pilots only under guardrails outlined by the Office of the Privacy Commissioner (OPC) of Canada. Keep data retention minimal and purpose-of-use explicit. Harden the vendor mesh: require secure, time-bound remote access and signed software updates wherever partners touch diagnostic systems, medical devices, or building controls.

Get informed, align on a unified plan, and practice together. Engage peers and regulators, share lessons, and run converged exercises with clinical leaders and facilities teams. Seek out guidance from user groups, conferences, and experts in the cybersecurity sector.

As I mentioned in CCN's recent report on OT cybersecurity, public safety and human lives depend on system integrity. When my child's life was in the hands of our local hospital, I understood what trust in healthcare truly means. Trust in healthcare doesn't end at the bedside, it extends to every system that keeps care running. Cybersecurity is how we protect that trust and safeguard lives when it matters most.

Enza Alexander is Executive Vice-President at ISA Cybersecurity, one of Canada's leading cybersecurity services and solutions providers. Enza is a seasoned IT industry leader with over 30 years of experience across the technology sector. She is passionate about helping clients understand how strong information security management systems can keep them cyber safe. Her extensive experience in the energy, utility, and healthcare sectors forms the foundation of her operational technology (OT) expertise.

In 2022, Enza was named one of Canada's Top Women in Cybersecurity by IT World Canada (ITWC) and a trailblazer woman leader by *Aspioneer Magazine*. In 2011, Enza was recognized as one of Canada's leading Women in Technology by IT Canada and *CDN Magazine*.

**CCN Quick Tips**

**Top 5 Cybersecurity Tips for Healthcare Workers**

**4. Handle Patient Data Securely**
Share information only on a need-to-know basis. Use approved secure channels, double-check recipients, and never discuss patient details in public areas.

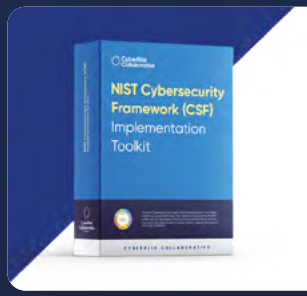
CyberRisk Collaborative
A CRA Resource

# Cybersecurity Framework Implementation Guides for NIST CSF and ISO27001/2



**CyberRisk Collaborative provides concise, framework-aligned guidance for healthcare cybersecurity teams to align, track progress, and keep audits moving forward.**

**Now available!** CyberRisk Collaborative (CRC) now provides one-time download cybersecurity framework toolkits that help organizations create clarity fast, so teams align on priorities, communicate progress, and sustain momentum.




The **NIST Cybersecurity Framework (CSF) Implementation Toolkit** helps healthcare organizations align their cybersecurity programs with both HIPAA Security Rule requirements and industry best practices, all while improving their ability to identify, protect, detect, respond, and recover from cyber incidents.

- Over **75 tools**
- Estimated cost savings of **$39,000 - $102,000** in consulting costs
- Based on a range of **$75-$150** per hour for a single FTE


The **ISO 27001/2 Framework Implementation Toolkit** empowers healthcare providers and business associates to formalize their information security management system (ISMS), demonstrating due diligence to patients, partners, and regulators.

- Over **85 tools**
- Estimated cost savings of **$56,000 - $147,000** in consulting costs for $7,500
- Based on a range of **$75-$150** per hour for a single FTE

**Start**
Buy individual toolkits.

**Equip**
Access guidance for **NIST CSF** & **ISO 27001/2**.

**Standardize**
Align teams, clarify scope/ applicability, report progress consistently.

**Get the Toolkits**

CyberRisk ALLIANCE

CyberRiskCollaborative.com

# Cybersecurity and Privacy in Canadian Healthcare: Navigating Critical Challenges in the Digital Age

by André Allen

The digitization of healthcare has revolutionized patient care delivery across Canada. It enables unprecedented access to medical records, streamlined treatment protocols, and enhances care coordination. However, this digital transformation also exposes the sector to significant cybersecurity and privacy vulnerabilities, risks that threaten patient safety, institutional reputation, and regulatory compliance. As healthcare organizations increasingly rely on interconnected systems and digital infrastructure, the imperative to protect sensitive health information has never been more critical.

## The Growing Threat Landscape

Canadian healthcare organizations face a growing cybersecurity crisis. The sector has become an increasingly attractive target for cybercriminals due to the high value of health information and the critical nature of healthcare operations. The COVID-19 pandemic accelerated digital transformation initiatives while simultaneously creating new vulnerabilities as organizations rushed to implement remote work solutions and telehealth platforms.

According to IBM's *2023 Cost of a Data Breach Report*, "Healthcare organizations experienced the highest average cost of a data breach for the 13th consecutive year, with an average cost of USD $10.93 million."[1] While this figure represents global data, Canadian healthcare organizations face similar financial pressures, as breaches often cost anywhere from $5 to 15 million depending on the scope and nature of the incident.

The Canadian Centre for Cyber Security has identified healthcare as a critical infrastructure sector facing heightened cyber threats. In its *2023 National Cyber Threat*

*Assessment*, the agency noted that "ransomware continues to be the cyber threat activity most likely to affect Canadians and Canadian organizations."[2] Healthcare organizations are particularly vulnerable to ransomware attacks due to the need for continuous system availability and often-outdated IT infrastructure.

### Real-World Examples and Consequences

Several high-profile incidents illustrate the severity of cybersecurity challenges facing Canadian healthcare. In October 2021, Newfoundland and Labrador's health authority experienced a significant cyberattack that affected the entire healthcare system of the province. The incident forced the cancellation of thousands of medical appointments and procedures, and some services took months to fully restore. Exact recovery costs have not been publicly disclosed, but similar incidents in other jurisdictions suggest costs in the tens of millions of dollars.

The 2021 cyberattack on Humber River Hospital in Toronto demonstrated how quickly healthcare operations can be disrupted. The hospital was forced to implement emergency protocols and revert to manual processes for several days while systems were restored. This incident highlighted the critical dependency healthcare organizations have on digital infrastructure for patient care delivery.

More recently, in 2022, the Sobeys pharmacy experienced a cyberattack that affected prescription services across multiple provinces, demonstrating how cyber incidents can impact healthcare service delivery beyond traditional hospital settings.

These examples underscore a fundamental challenge, as healthcare organizations operate in an environment where system availability directly impacts patient safety. Unlike other sectors, where brief downtime may cause inconvenience, healthcare cyber incidents can compromise patient care and potentially endanger lives.

### Regulatory Framework and Compliance Challenges

Canadian healthcare organizations must navigate a complex regulatory landscape governing privacy and cybersecurity. The *Personal Information Protection and Electronic Documents Act (PIPEDA)* establishes baseline privacy requirements for federally regulated organizations, while provincial health information acts impose additional obligations specific to health data. For example, Ontario's *Personal Health Information Protection Act (PHIPA)* requires healthcare organizations to implement appropriate administrative, technical, and physical safeguards to protect personal health information.

The Office of the Privacy Commissioner of Canada has emphasized the importance of cybersecurity in protecting personal information. In its guidance documents, the office notes that "organizations have a legal obligation under PIPEDA to protect personal information with security safeguards appropriate to the sensitivity of the information."[3]

Sobeys pharmacy experienced a cyberattack that affected prescription services across multiple provinces.

Compliance costs are substantial and continue to grow. Healthcare organizations typically allocate 10–15% of their IT budgets to cybersecurity and privacy compliance initiatives. However, these investments often fall short of addressing evolving threats, as cybercriminals continuously develop new attack methods and exploit emerging vulnerabilities.

### Mitigation Strategies and Best Practices

Effective cybersecurity in healthcare requires a multi-layered approach that addresses technical, administrative, and physical safeguards. Leading healthcare organizations are implementing comprehensive cybersecurity frameworks based on recognized standards such as the NIST Cybersecurity Framework and ISO 27001.

**Risk Assessment and Management:** Regular vulnerability assessments help identify potential weaknesses before they can be exploited. The Canadian Centre for Cyber Security recommends that organizations "conduct regular risk assessments to identify, analyze, and evaluate cyber security risks."[4] Healthcare organizations should implement continuous monitoring and conduct comprehensive security assessments at least annually.

**Employee Training and Awareness:** Human error remains a leading cause of healthcare data breaches. The *2023 Verizon Data Breach Investigations Report* found that "74% of all breaches include the human element."[5] Comprehensive training programs that include simulated phishing exercises and regular security awareness updates are essential for reducing this risk.

**Network Segmentation and Access Controls:** Implementing zero-trust architecture principles helps limit the spread of cyber attacks. This includes segmenting networks to isolate critical systems, enforcing multi-factor authentication, and regularly reviewing user access privileges. The principle of least privilege should be applied consistently across all systems and user accounts.

**Incident Response Planning:** Comprehensive incident response plans enable organizations to respond quickly and effectively to cyber threats. These plans should include clear communication protocols, legal notification requirements, and recovery procedures. Regular testing and updating of these plans is essential to ensure their effectiveness during actual incidents.

## The Role of Legal Expertise in Healthcare Cybersecurity

The intersection of healthcare, technology, and law creates complex challenges that require specialized expertise. Legal professionals with a deep understanding of cybersecurity requirements and healthcare regulatory obligations play a crucial role in helping organizations navigate these challenges effectively.

Healthcare clients often struggle to balance operational efficiency with security requirements, particularly when implementing new technologies or responding to cyber incidents. Legal guidance becomes essential in areas such as vendor contract negotiations, breach notification requirements, and regulatory compliance strategies.

The legal landscape continues to evolve as regulators adapt to emerging threats. Healthcare organizations need legal partners who stay current with these developments and can provide practical guidance on implementation. This includes understanding the nuances of provincial health information legislation, federal privacy requirements, and emerging cybersecurity regulations.

Contract negotiations with technology vendors present particular challenges in healthcare. Standard software licensing agreements often include liability limitations that may not adequately protect healthcare organizations in the event of a cyber incident. Legal review and negotiation of these agreements is critical. It ensures appropriate risk allocation and that security requirements are clearly defined and enforceable.

## Future Considerations and Emerging Challenges

The healthcare cybersecurity landscape continues to evolve rapidly. Emerging technologies such as artificial intelligence, Internet of Medical Things (IoMT) devices, and cloud-based health platforms introduce new vulnerabilities while offering significant benefits for patient care. Healthcare organizations must balance innovation with security, ensuring that new technologies are implemented with appropriate safeguards.

The Canadian government has recognized cybersecurity as a priority for national security. The *2019–2024 National Cyber Security Action Plan* emphasizes

the need to "secure vital cyber systems and services" and includes specific provisions for protecting critical infrastructure, including healthcare systems.[6]

Regulatory expectations are also increasing. Organizations should prepare for enhanced reporting requirements, mandatory security standards, and increased regulatory oversight. The cost of cybersecurity will continue to rise, but the cost of inadequate protection is far higher.

## Conclusion

Cybersecurity and privacy protection in Canadian healthcare require sustained commitment, adequate resources, and specialized expertise. When considering patient safety and financial consequences, the stakes are simply too high for organizations to approach these challenges without comprehensive strategies and qualified support.

Success requires collaboration between healthcare professionals, technology experts, and legal advisors who understand the sector's unique challenges. Organizations that invest proactively in cybersecurity and privacy protection not only reduce risk exposure but also position themselves to use digital technologies more effectively to improve patient care.

The path forward demands vigilance, investment, and expertise. Healthcare organizations that recognize cybersecurity and privacy as fundamental enablers of quality patient care, rather than mere compliance obligations, will be best positioned to thrive in an increasingly digital healthcare environment. This approach ensures sensitive information remains protected while supporting innovation and trust.

See end notes for this article's references.

Note: While these sources represent the most current and reliable information available, readers should verify specific statistics and consult current government and industry reports for the most up-to-date information, as cybersecurity data and regulatory requirements continue to evolve rapidly.

André Allen is the Chief Information Security Officer (CISO) and a Director, Cyber and Technology Enablement, at INQ Consulting. With more than 30 years of Technology experience, Andre was formerly the CIO & CISO at Algoma University and previous to that Vice President of IT at MaRS Discovery District, where he served as Chief Information Security Officer and Chief Privacy Officer. With more than 25 years of experience leading diverse technology teams, André has led significant ERP, privacy and cybersecurity strategy and implementation projects and is well versed in both the infrastructure and architecture of AI, cyber security, and data management.

# RED X CARBON

## THE CLOUD MASTERS

## INNOVATION THAT'S SECURE BY DESIGN

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Infrastructure
Azure

At the core of our mission is Security—driving trust, resilience, and performance.

We specialize in:

- **Data & AI**: Unlocking insights with intelligence
- **Infrastructure**: Building scalable, secure foundations
- **Digital & App Innovation**: Creating transformative experiences

***Together, we shape a future where technology works SMARTER and SAFER.***


www.redxcarbon.com
sales@redxcarbon.com
1-866-733-9227


ISO 27001:2022

bsi ISO/IEC 27001 Information Security Management CERTIFIED

# A Field Guide for Short-Staffed Teams: Securing Healthcare in a Digital Age

by Terry Cutler

## Executive Summary

Healthcare is under nonstop fire. I'm often called onto TV when there's a breach: ransomware, account takeovers, insider mistakes, exposed patient data in shared drives, you name it. The hospitals I advise, some with 8,000 to 18,000 endpoints, faces similar stories and challenges. They're short-staffed IT, under tight budgets, and pressure to "DIY" a Security Operations Center (SOC) or Network Operations Center (NOC) without the time, money, or specialist skills to do it right. So they mix and match tools that weren't designed to work together, and too often, we end up with10 people on a Zoom call trying to piece together what just happened.

Working in the trenches with IT, I get to see their pain and frustration, and I want their leadership to see it too. This article offers a practical, low-friction way to measurably reduce risk in 90 days, without trying to hire a unicorn team or build a 24/7 SOC from scratch. You'll learn what to audit, what to fix first, how to get executive buy-in, and how to prove progress with simple metrics.

## 1. Reality on the Ground

Healthcare IT is chronically short-staffed. Your best system administrator often becomes the "temporary" security analyst, buried in tickets and 500-page risk reports. Every dollar must show patient-care impact, so tools without clear outcomes get cut. Leadership loves the idea of "our own SOC," but what you usually end up with is a poorly configured Security Information and Event Management (SIEM) system that generates alert fatigue and blind spots. Add Electronic Health Records (EHR), imaging systems, Internet of Medical Things (IoMT), contractors, and data moving everywhere, and it's no wonder hospitals struggle. It's not apathy, it's an impossible job without clear priorities, automation, and human expertise working together.

## 2. Why DIY SOC/NOC Fails

A real SOC is more than big screens. It's 24/7 monitoring, tuned detections, active threat hunting, forensic analysis, and compliance mapping (ISO 27001, NIST CSF, CIS Controls, PIPEDA/PHIPA/Law 25). Trying to do that with a skeleton crew turns expensive tools into shelfware. Most hospitals succeed by combining automated detection and response with a trusted SOC partner while maintaining in-house oversight for accountability.

## 3. The 90-Day Stabilization Plan

**PHASE 0 – GET PREPARED:**

Find an executive sponsor who can cut red tape. Pick 3–5 outcome metrics leadership will care about (risk score, unsupported endpoints, leaked accounts). Pause risky infrastructure changes until after your audit.

**PHASE 1 – RAPID REALITY-CHECK CHALLENGE AUDIT:**

In hours, not months, you can collect event logs, patch history, password and lockout policies, endpoint posture, failed login data, and dark web leaks. Then flag unsupported or legacy devices, unencrypted Protected Health Information (PHI) in shared drives, and weak account hygiene. Deliver a simple executive summary, "report card," and prioritized fix plan to the management team.

**PHASE 2 – HARDENING & ACCESS CONTROL:**

Close the easy doors first: enable Multi-Factor Authentication (MFA) everywhere, remove stale or shared accounts, enforce lockouts and strong passwords, patch critical systems, segment IoMT and Operational Technology (OT) from business and EHR networks, block risky web categories, and set a real patch schedule.

**PHASE 3 – DETECTION & RESPONSE:**

Deploy Endpoint Detection and Response (EDR) with auto-containment, tune SIEM rules to cut noise, and add 24/7 managed monitoring so someone's awake when you're not. Run a quick ransomware drill to test detection, isolation, communication, and recovery.

**PHASE 4 – RESILIENCE & PROOF:**

Lock in backups that are offline or immutable and test them for real. One of the simplest and still most effective backup strategies is the 3-2-1 rule. Keep three copies of your data (the live version and two backups), store them on two different types of media (for example, local server storage plus an external drive or cloud), and make sure one copy is off-site and offline where attackers can't reach it. That offline copy could be a cloud backup with immutability turned on or a disk/tape that's physically disconnected. This matters in healthcare because if ransomware encrypts both your production systems and any network-attached backups, as they typically do, the offline/off-site copy stays safe. Using different media lowers the risk of a single point of failure such as a drive crash or fire, and multiple copies protect against user error, corruption, or malware.

Next, tighten email security (DMARC/DKIM/SPF). Review administrative and service accounts for least privilege. Simulate downtime of Electronic Medical Record (EMR) systems or imaging systems to confirm patient care continues. Finally, return to your original metrics and prove risk has dropped.

## 4. The "Don't Skip" Control Set

If you can't do everything, nail this minimum-viable stack:

1. **Identity & Access:** MFA everywhere, strong passwords, lockouts, no orphaned temporary accounts.
2. **Endpoints & Email:** EDR with tamper protection, application allow-listing on kiosks, strong phishing defenses, and ongoing staff training.
3. **Network Hygiene:** Segment clinical gear, block risky outbound traffic, monitor DNS, disable direct Remote Desktop Protocol (RDP), protect VPN with MFA.
4. **Patch Discipline:** Own update schedules, patch high-risk systems first, add compensating controls for legacy gear.
5. **Data Protection:** Know where PHI and Personally Identifiable Information (PII) lives, reduce shared drive sprawl, and back it up using a tested 3-2-1 strategy.
6. **Detection & IR:** Centralize and tune logs, add 24/7 threat monitoring, and run at least one tabletop drill so leaders know their roles.
7. **Governance & People:** Map to NIST/CIS, stay compliant with PIPEDA/PHIPA/Law 25, brief executives in plain language, and build a no-shame reporting culture.

## 5. Budget-Smart Roadmap

- **GOOD (Start Now):**

  Run a Cybersecurity Reality Check Challenge, a safe mini-penetration test to reveal detection gaps. Lock down MFA, account hygiene, EDR, patch plans, and backups (test restores). Block risky webmail to stop ransomware from sneaking in through personal accounts.

- **BETTER (60–120 Days):**

  Segment IoMT/OT, centralize and tune alerting, add 24/7 monitoring, deploy Domain-based Message Authentication, Reporting, and Conformance (DMARC) to stop spoofing, tighten privileged access, and ramp up positive phishing awareness.

- **BEST (6–12 Months):**

  Build and run full incident response playbooks with clinical leadership, automate patching, deploy Data Loss Prevention (DLP) and encryption for PHI, expand threat hunting, and test business continuity under real clinical workflows.

## 6. Show Executives the Right Metrics

When you're talking to executives, remember this: they're not buying cool tech. They're buying reduced clinical risk, fewer lawsuits, and smoother patient care, even as IT takes the hits. If you want them to keep funding security, speak their language, not ours.

Skip the technobabble and dashboards that only a SOC analyst loves. Show how your work keeps patients safe, critical systems running, and the hospital out of the headlines. Frame the story around business continuity and legal risk, not SIEM rules or firewall configurations.

A great way to do this is with a simple, business-focused scorecard with no more than one slide delivered every couple of weeks. Pick a handful of metrics that anyone on the executive team can understand at a glance:

- **Risk trend:** Overall risk score since the last audit.
- **Detection speed:** How fast you can now isolate an infected device (minutes vs. hours).
- **Credential safety:** Number of leaked staff accounts found and secured.
- **Patch coverage:** Percentage of endpoints now running supported, fully patched operating systems.
- **Resilience:** Date and success of the last restore test of a key clinical system (and how close you are to your recovery objectives).
- **Continuity impact:** Estimated downtime avoided or costs saved when an incident was contained.
- **Compliance exposure:** Progress toward key frameworks (NIST CSF, CIS Controls) and laws like PIPEDA, PHIPA, Law 25—especially anything that shrinks fine or lawsuit risk.

Keep each point to a single, clear sentence describing impact:

*Reduced leaked-credential exposure from 243 to 31 accounts, cutting the chance of email takeover and prescription fraud.*

I*mproved ransomware isolation time from 3 hours to 15 minutes, protecting clinical care continuity.*

This style of reporting keeps the conversation focused on patient safety, uptime, compliance, and cost avoidance. It's really all the things the C-suite actually cares about. Show that every dollar invested is making attacks less likely and less damaging, you'll keep leadership engaged and backing your roadmap.

## 7. Common Failure Patterns

- **DIY SOC Trap:** Untuned SIEMs miss about 79% of MITRE ATT&CK techniques and become a $200K doorstop without 24/7 analysts.
- **Personal Webmail:** Bypasses corporate email defenses and lets ransomware in.
- **No Lockouts:** Attackers brute-force all weekend.
- **Zombie Endpoints:** Forgotten XP/kiosk machines become backdoors.
- **Failed Login Noise:** Thousands of failed login attempts go unnoticed.
- **PII Everywhere:** PHI scattered across shared drives triggers Law 25/PHIPA breach notices.

## 8. The Hybrid Model: Automation + Human Expertise

Hospitals that stay ahead don't try to hire a full Hollywood cast of security unicorns. They blend smart automation with seasoned human expertise to get speed, scale, and clinical reality—without building a 200-person SOC they can't afford.

Automated discovery and risk scoring give teams a clear, accurate picture fast of what's exposed, what's vulnerable, and what to fix first. Managed detection and response that actually acts at 2 a.m. means an infection can be contained before it spreads. Senior security advisors (vCISO-style) turn raw findings into policies, budgets, and training leadership can understand and support.

This hybrid approach avoids the nightmare of trying to hire five rare specialists you'll never keep. It still giving executives what they want most: visibility, assurance, and proof that security dollars are reducing real risk.

## Bringing It All Together

You don't need a 200-person security team. You need a focused plan, the right first fixes, and partners who can act at 2 a.m. when ransomware hits a nurse's station.

If you want sample reports or a quick walk-through, grab 30 minutes with me at www.TalkToTerryCutler.com and I'll show you what we usually find in the first week and how to get your risk trending down immediately without adding headcount you can't afford to hire.

Stay safe out there.

Terry Cutler is the CEO of Cyology Labs, a Controlled Goods Certified cybersecurity firm, and the author of the #1 Amazon Best Seller *Insider Secrets to Internet Safety: Advice from a Professional Hacker.* As an international award-winning cybersecurity expert and government-cleared ethical hacker, Terry is trusted by businesses, law enforcement, and defense contractors alike to uncover threats, prevent breaches, and simplify complex cyber risks.

With over two decades of experience, Terry has helped some of Canada's largest organizations defend against internal and external attacks. His engaging approach has landed him on national TV, radio, podcasts, and stages across North America and the Middle East, where he delivers eye-opening insights and live hacking demos that expose how cybercriminals exploit human and technical weaknesses.

ASSURANCE IT

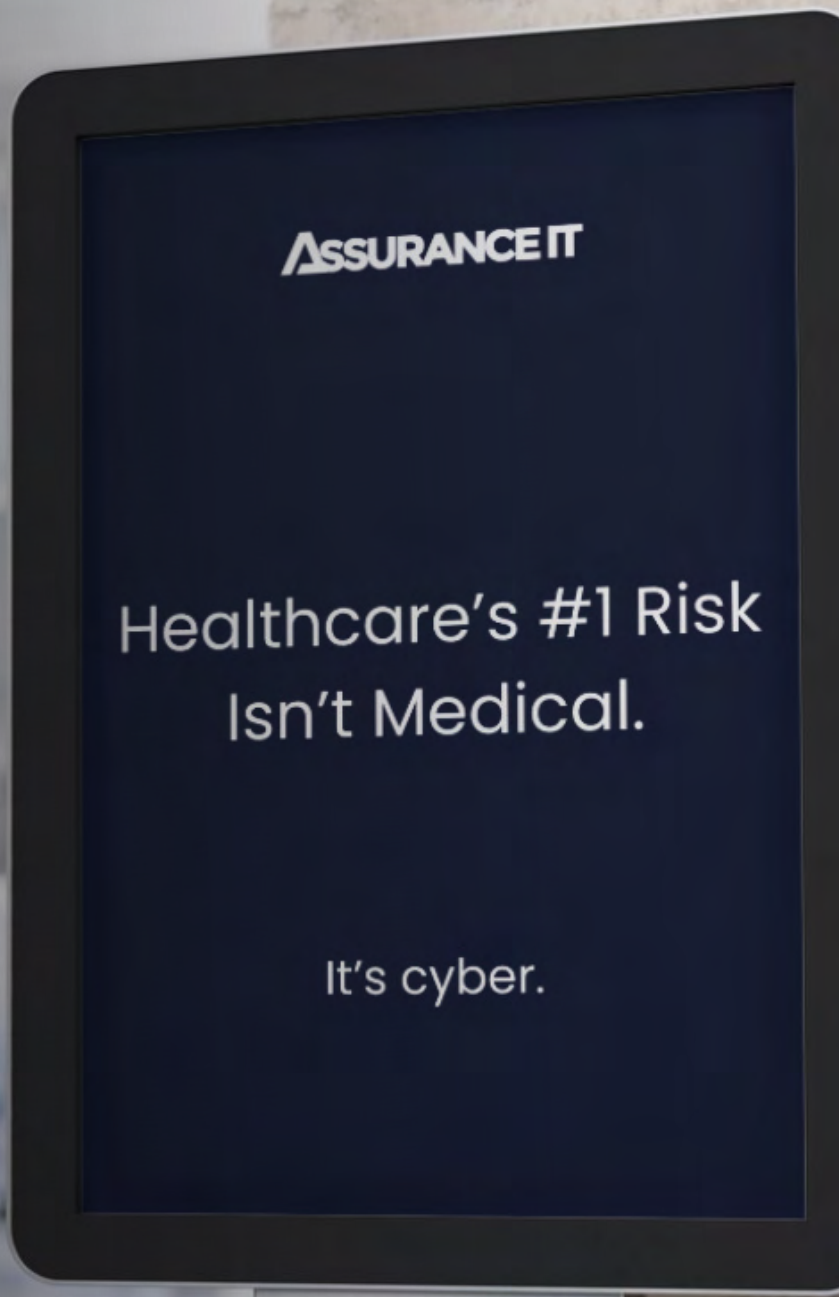
*Next Gen MSSP*

# No power.
# No records.
# No care.

## $9.77M
**Cost of a breach**

## +92%
**Hit last year**

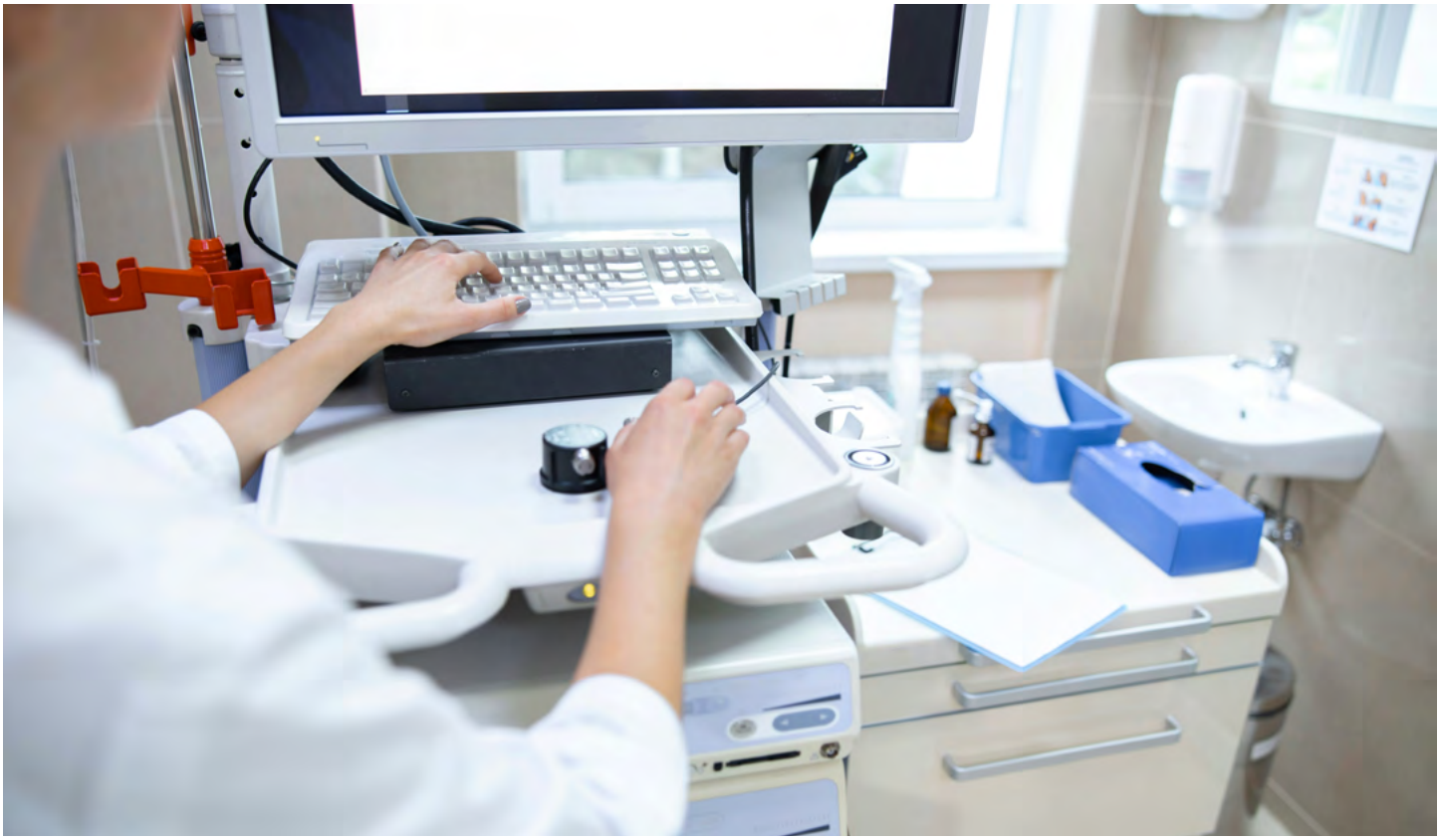
## 50X
**More valuable than financial data**




**Contact Us**

514-357-5399
1 (877) 892-3399

Info@assuranceit.co
AssuranceIT.co



# Why Every Healthcare Worker Is Now on the Cybersecurity Frontline

by François Guay

## Introduction

In Canada's hospitals and clinics, protecting patients now extends far beyond medicine. As healthcare grows increasingly digital through electronic health records, telemedicine, and connected medical devices, so too does its exposure to cyberattacks. From canceled surgeries in Ontario to delays at a leading pediatric hospital, cyber incidents are no longer hypothetical. They are disrupting real care.

Cybersecurity is no longer the sole responsibility of IT specialists. Every healthcare worker, from physicians to clerical staff, now stands on the cybersecurity frontline.

## Rising Cyber Threats to Healthcare

Healthcare has become one of the most targeted sectors for cybercrime worldwide. Unlike financial data that can be reset, medical records are permanent, deeply personal, and highly valuable on the dark web. And because hospitals cannot afford downtime, attackers see them as prime targets for ransoms.

The Canadian Centre for Cyber Security (Cyber Centre) reported a 75% increase in ransomware attacks against healthcare between 2022 and 2023 (Canadian Centre for Cyber Security 2023). Globally, 2024 set a record for healthcare breaches, with more than 276 million patient records exposed (Cybersecurity News 2025). The average cost of a healthcare breach remains the highest among industries, often in the tens of millions (HIPAA Journal 2025).

Ransomware dominates the threat landscape. Over 90% of attacks begin with phishing, an email, text, or call tricking an employee into opening the door (Healthcare Facilities Today 2025). Criminal groups exploit the human element because it is far easier to deceive a person than hack an encrypted server. The stakes are no longer abstract. For

healthcare leaders, cyber risk now sits alongside clinical risk and the decision they make today will shape patient safety tomorrow.

## When Cyberattacks Hit Home

Canada has already seen the damage firsthand:

- **Ontario, 2023:** Hackers infiltrated the IT services provider for five hospitals in southwestern Ontario. The Daixin ransomware forced the shutdown of digital systems, leading to canceled surgeries, delayed appointments, and emergency "Code Grey" declarations. Data from 5.6 million patient visits was stolen, affecting more than 326,000 patients (CBC News 2023; Global News 2024). Recovery took months.
- **SickKids, 2022:** Toronto's Hospital for Sick Children (SickKids) faced a ransomware attack from the LockBit gang, causing diagnostic and treatment delays. In an unusual twist, LockBit apologized and released a free decryption key, claiming children's hospitals were off-limits. Even so, the attack exposed the fragility of pediatric care when systems fail (CBC News 2023; Control Engineering 2023).
- **Newfoundland & Labrador (NL), 2021:** A ransomware breach brought down the province's entire healthcare network, halting thousands of appointments and forcing staff back to pen-and-paper. The incident cost $16 million to investigate and remediate, showing the scale of disruption when an entire province's health system is paralyzed (Government of NL 2023).

These Canadian cases mirror global crises. In the UK, the 2017 WannaCry ransomware infected one-third of National Health Service (NHS) hospitals, forcing ambulance diversions and canceling an estimated 19,000 appointments (NAO 2017; MedTechNews 2025). In 2024, a breach at Change Healthcare in the U.S. compromised data for nearly 193 million people and froze billing systems nationwide (HIPAA Guide 2025).

The lesson is clear: whether local or international, healthcare cyberattacks directly endanger patients and destabilize entire health systems. For leaders, the question is no longer if—but how prepared are we for the next wave?

## The Human Factor: Weakest Link, First Defense

Technology alone cannot solve this problem. Most attacks succeed not because of technical flaws, but because of human behaviour. Verizon's global breach report found that nearly 70% of breaches involve a human element, such as an error, stolen credentials, or social engineering (Verizon 2024).

Healthcare workers are especially vulnerable. A busy nurse might click on what looks like a routine email. A doctor might reuse a weak password. A technician might plug an infected USB into a lab computer. Each of these everyday actions can unleash a hospital-wide crisis.

Phishing remains the top vector. One study found that 14% of healthcare employees click on simulated phishing emails, enough for attackers to gain a foothold (KnowBe4 2019). Even one misstep can compromise an entire network. But humans can also have the strongest defense. The same nurse who might click on a phishing link can, with the right training, recognize and report it—stopping an attack in its tracks.

## Awareness and Training: Progress and Gaps

Many Canadian hospitals now run annual security modules, phishing simulations, and policy refreshers. Horizon Health Network in New Brunswick demonstrates that persistent training works, reducing phishing click rates to under 3% and helping avoid major cyber-related downtime (Health Standards Organization 2023).

Yep gaps remain widespread. Surveys show that one-third of healthcare staff report receiving no cybersecurity training at all. Among those trained, many say it is too generic or infrequent. Nearly 32% skimmed their organization's security policy only once, and shockingly 1 in 10 managers don't know if their organization even has one (Kaspersky 2019).

What works best are short, role-specific, and frequent training sessions. Gamified e-learning, Canadian case studies, and unit-level "cyber champions" keep security relevant (Jerry-Egemba 2024; Click Armor 2024; Salama et al. 2024). Leadership buy-in also matters: when senior executives frame cybersecurity as patient safety, staff take it seriously. One-off compliance-driven modules fail since overwhelmed clinicians see them as checkboxes. Without daily reinforcement, lessons fade fast.

## Barriers to a Secure Culture

Despite recognition of the problem, barriers remain:

1. **Perception Gap:** Many staff still view cyber risks as an IT responsibility rather than a component of clinical safety.

2. **Workflow Friction:** Password resets, Multi-Factor Authentication (MFA), and complex systems often feel like obstacles to patient care.
3. **Exhaustion:** Long shifts and staff shortages lead to fatigue-driven mistakes that attackers exploit.
4. **Resource Gaps:** Smaller hospitals frequently operate outdated systems without 24/7 IT support.
5. **Device Chaos:** Personal devices and decentralized care environments add layers of complexity.
6. **Compliance Overload:** Cybersecurity rules are often buried among endless protocols, causing disengagement.

Unless these barriers are addressed, healthcare will remain exposed to preventable cyber risks.

## Building a Cyber-Aware Culture

A resilient defense requires turning every worker into a cyber ally. Key steps include:

- **Leadership & Culture:** Treat cybersecurity as patient safety and celebrate the reporting of mistakes rather than punishing them.
- **Shared Ownership:** Involve frontline staff in selecting secure apps and shaping policies so that rules make sense in clinical settings.
- **Continuous Training:** Replace annual modules with ongoing, short, role-based refreshers paired with phishing drills and immediate feedback.
- **Simplify Policies:** Focus on essentials: strong passphrases, MFA, and a clear reporting channel, make compliance intuitive.
- **Technology That Helps:** Provide tools that lighten the burden, flag suspicious emails, auto-encrypt data, and make secure apps easier than insecure workarounds.
- **Positive Reinforcement:** Highlight wins when staff prevent harm and celebrate "cyber heroes" just as infection-control champions are recognized.

Cybersecurity must become as natural and habitual as hand hygiene: constant, reinforced, and clearly tied to patient care.

## Every Worker Matters—Now More Than Ever

Cybersecurity is inseparable from patient safety. A ransomware attack can delay surgeries, divert ambulances, or leak intimate patient records. The flip side is equally true: one alert clerk or nurse can stop an entire crisis before it begins. Healthcare leaders must invest in training, practical policies, and supportive tools. Governments and industry must ensure resources flow even to small clinics. Most importantly, organizations must embed cyber vigilance into daily routines, and not treat it as an annual compliance task.

The path forward is empowerment. Every healthcare worker, executive, doctor, nurse, or support staff, must be equipped to act as a guardian of patients and their data. Together, technology and human vigilance can create a healthcare system resilient against the growing wave of cyber threats.

The frontline is everywhere: in every hospital corridor and clinic office. And today, every healthcare worker stands on it, ready or not.

See end notes for this article's references.

François Guay is the visionary founder of Canada's largest cybersecurity network, the Canadian Cybersecurity Network (CCN), which unites over 44,000 members from diverse sectors, including individuals, businesses, universities, professional associations, diversity groups, and government agencies, representing nearly 1,000,000 people across the country. Under François's leadership, CCN has become a cornerstone in fostering collaboration, innovation, and security in Canada's rapidly evolving cybersecurity ecosystem.

### CCN Quick Tips

**Top 5 Cybersecurity Tips for Healthcare Workers**

**5. Stay Alert and Report Quickly**

Complete security training, stay aware of current threats, and report any suspicious activity or mistakes right away — early reporting can stop a small slip from becoming a major breach.

## stay connected

# SPONSOR OUR 2026 REPORTS

State of Cybersecurity (Jan)
Agentic AI & Cyber (April)
National Defense & Cyber (Sept)

# Conclusion & Recommendations

*The Pulse Check: National Cybersecurity in Healthcare 2025* report exposes a critical truth: the greatest threats to Canada's healthcare system is no longer limited to outbreaks or new illnesses, it is the risk of failing to act on cybersecurity. Digital transformation has outpaced digital protection, and the cost shows up in delayed treatments, breached data, and eroded public trust. Cybersecurity can no longer be treated as an IT issue or a compliance checkbox. It is now a core pillar of patient safety, every bit as essential as sterile instruments or clean operating rooms.

## The Human Factor Defines Success

Every insight in this report leads to the same conclusion: technology alone cannot secure healthcare. True resilience depends on the people who deliver care, manage systems, and make everyday decisions. From recognizing phishing attempts to demanding secure procurement, awareness and accountability must be embedded into the culture of care itself. If cybersecurity isn't human-centric, it won't succeed.

## Canadian Cybersecurity Network's (CCN) National Recommendations

As Canada's largest cybersecurity community, the CCN calls for decisive, coordinated action built on five national imperatives:

1. **Recognize cybersecurity as a patient safety issue**
   Embed cybersecurity into every healthcare policy, accreditation standard, and funding decision as a core component of clinical safety and quality of care.
2. **Establish a national framework for healthcare cyber resilience**
   Develop a national framework with harmonized minimum standards for hospitals, clinics, and health authorities, supported by dedicated funding and measurable outcomes.
3. **Invest in people, not just products**
   Expand national training and workforce programs in healthcare cybersecurity and strengthen pathways to recognized professional certifications. For those in the field, set them up for success through ongoing, role-specific awareness and simulation-based learning.
4. **Create a permanent national threat intelligence exchange**
   Build a collaborative model, like the one pioneered by CCN, to connect hospitals, vendors, and government agencies for real-time sharing of threat data, playbooks, and lessons learned.
5. **Adopt secure-by-design procurement and funding models**
   Tie public funding and digital-health investments to verifiable security criteria, conformance testing, and lifecycle requirements, from procurement through decommissioning, by utilizing existing toolkits and programs (e.g., Infoway privacy/security requirements, provincial operating models, and federal certification regimes).

## A National Moment of Decision

Canada has the talent, technology, and leadership to build one of the world's most cyber-resilient healthcare systems, but only if we act now. The path forward calls for collaboration over competition, investment over improvisation, anchored in a people-first mindset that sees every healthcare worker as a guardian of patient trust.

This report is not an ending; it's a call to action. Cybersecurity is no longer about firewalls and endpoints. It's about people, trust, and the continuity of care that defines who we are as a nation. Protecting Canada's digital healthcare is protecting the heartbeat of Canada itself.

# References


**Cybersecurity: The New Health Care Emergency in Canada** by Elias Diab, Presented by Accerta

Charles Eckert, Partner, Cybersecurity, Privacy and Financial Crime, PwC Canada, and Justin Abel, Partner, PwC Canada. The emerging cyber-security risks facing Canada's public sector: How government and public-sector leaders can foster cyber resilience while laying the foundation for new citizen services.

**Securing the Front Lines of Care: Why Cyber Resilience Is Essential to Modern Healthcare in Canada** by Serge Charette, Presented by Tanium

Claroty. State of CPS Security: Healthcare Exposures 2025. Claroty, 2025.

Nova Scotia Auditor General. Report on Digital Health Network Security. Halifax: Office of the Auditor General of Nova Scotia, October 2024.

MITRE Corporation. Known Exploited Vulnerabilities Catalog. MITRE, 2025.

CVE Program. CVE Vulnerability Statistics. CVE, 2025.

Cybersecurity and Infrastructure Security Agency (CISA). Threat Exploitation Trends and AI Acceleration. CISA, 2025.

Government of Canada. Bill C-72: Connected Care for Canadians Act. Ottawa: Parliament of Canada, 2024.

Government of Canada. Bill C-8: Critical Cyber Systems Protection Act. Ottawa: Parliament of Canada, 2024.

Government of Québec. Law 5: Act Respecting Health and Social Services Information. Québec City: National Assembly of Québec, July 2024.

**Cybersecurity and Privacy in Canadian Healthcare: Navigating Critical Challenges in the Digital Age** by André Allen

[1] IBM Security. "Cost of a Data Breach Report 2023." IBM Corporation, 2023.

[2] Canadian Centre for Cyber Security. "National Cyber Threat Assessment 2023-2024." Communications Security Establishment, 2023.

[3] Office of the Privacy Commissioner of Canada. "Privacy and Cyber Security."

[4] Canadian Centre for Cyber Security. "Cyber Security Risk Management." Communications Security Establishment.

[5] Verizon. "2023 Data Breach Investigations Report." Verizon Enterprise, 2023.

[6] Government of Canada. "National Cyber Security Strategy 2019-2024." Public Safety Canada, 2022 Update.


Note: While these sources represent the most current and reliable information available, readers should verify specific statistics and consult current government and industry reports for the most up-to-date information, as cybersecurity data and regulatory requirements continue to evolve rapidly.

# References

## Why Every Healthcare Worker Is Now on the Cybersecurity Frontline by François Guay


Canadian Centre for Cyber Security. 2023. National Cyber Threat Assessment 2023–2024. Ottawa: Government of Canada.

CBC News. 2023. "Southwestern Ontario Hospitals Hit by Ransomware Attack." December 2023.

Control Engineering. 2023. "LockBit Issues Apology After SickKids Attack." January 2023.

Cybersecurity News. 2025. "Healthcare Cyber Attacks Reach Record Levels." May 2025.

Global News. 2024. "Ontario Hospital Cyberattack Impact and Recovery." February 2024.

Government of Newfoundland and Labrador. 2023. "Cybersecurity Incident Report." St. John's: Government of NL.

Healthcare Facilities Today. 2025. "Report: Healthcare Ransomware Attacks Up 21 Percent in 2024." May 2025.

Health Standards Organization. 2023. "Horizon Health Network Cybersecurity Training Success." Ottawa: HSO.

HIPAA Journal. 2025. "2024 Healthcare Data Breach Report." January 2025.

HIPAA Guide. 2025. "Change Healthcare Breach Affects 192 Million Individuals." March 2025.

Jerry-Egemba, Uche. 2024. "Gamification in Cybersecurity Training for Healthcare." Journal of Health IT Security.

Kaspersky. 2019. "Healthcare Cybersecurity Training Gaps." Kaspersky Security Bulletin.

KnowBe4. 2019. "Phishing Simulation Benchmarks for Healthcare." Clearwater: KnowBe4.

MedTechNews. 2025. "WannaCry Lessons for Healthcare Cybersecurity." April 2025.

NAO (National Audit Office). 2017. "Investigation: WannaCry Cyber Attack and the NHS." London: NAO.

Salama, Ahmed, et al. 2024. "Role-Based Cybersecurity Training in Clinical Settings." Canadian Health Informatics Review.

Verizon. 2024. Data Breach Investigations Report (DBIR). New York: Verizon.


ccn