

POLICY BRIEF

CSA Z8005:24 Special requirements for digital infrastructure and digital health technologies in Canadian health care facilities

Connecting CSA Standards to Public Policy

July 2025



Overview

- **Canadian Standards Association (CSA Group) has developed a standard to provide guidance on digital infrastructure and digital health care technologies used in health care facilitie**s (HCFs). The standard is designed for use in all types of health care facilities, ranging from major public hospitals to small rehabilitation clinics.
- **Adopting digital infrastructure standards can help to support HCFs in securely leveraging health technologies** to enhance diagnostic efficiency, optimize service delivery, facilitate clinical innovation, and improve the health care experience for both patients and staff.
- The new CSA Z8005:24 Standard complements pan-Canadian efforts to embrace digital health practices, including electronic health records. **Secure, scalable, high-capacity digital infrastructure** across a critical mass of health care facilities is **an important milestone** in achieving Canada's seamless digital health care goals.
- **Provincial and territorial governments play a crucial role** as leaders and funders in digital health: particularly by incentivizing future-readiness, interoperability, and security in health care delivery.

Why a standard is needed

Digital technologies are transforming health care across Canada; however, HCFs of all sizes are facing challenges in keeping pace with rapid and fragmented technological change.

Digital transformation in health is often unplanned and uneven.[1] In many Canadian health care facilities, **fax machines sit alongside AI-enabled diagnostic devices.** Both need to be able to "plug into" the overall digital infrastructure — literally and metaphorically — and operate in tandem with the hundreds of other technologies that keep HCFs running.

Without effective coordination and planning, HCF investments in technological solutions and digitization can result in even higher costs, including lost time, administrative burdens, and compromised patient outcomes. Several recent incidents in Canada, including cyberattacks that have compromised data for millions of patients, have reaffirmed to health care leaders that their facilities need strong, secure digital infrastructure to deliver quality care and maintain patient trust.



It is challenging for HCF administrators and sector leaders to find **practical guidance on the best implementation strategies** for digital health technology and how to responsibly integrate new tools into their existing digital infrastructure.[1] **CSA facilitated the development of CSA Z8005:24 to address this gap** and provide much-needed guidance on digital infrastructure that is specific to Canadian HCFs.

Digital health in Canada: a changing landscape



- Canada was ranked only 18th of 32 high-income countries in the 2024 World Index of Healthcare Innovation, and even lower (20th) for health digitization specifically.
- In a recent survey, **80%** percent of Canadians said that they believe that investing in health care technologies should be a top priority for the government.
- In a 2024 survey of physicians, **68%** of respondents reported spending over an hour each day searching for patient information necessary for care.

1 **Angus, M., Byczko, C., Grossman, G., Munro, R., Murthy, P., Parypa, B.** (2021). Deployment of Health Care Facility Digital Infrastructure in Canada. A Framework for Standard-Based Solutions. Canadian Standards Association, Toronto, ON.

About the CSA Z8005:24 Standard

Developing the Standard

CSA Z8005:24 (the Standard) was created in consultation with experts across the health care system such as hospital administrators, public health authorities, architects, health system planners, health care infrastructure specialists, cybersecurity experts, and health care technology engineers.



The development of the Standard was made possible with financial support from the governments of all thirteen provinces and territories, as administered by Canada's Drug Agency (CDA-AMC), formerly the Canadian Agency for Drugs and Technologies in Health (CADTH).

Standard requirements vs. recommendations

The Standard includes provisions that, if implemented, HCFs are required to follow, as well as other provisions that are recommendations or suggestions. The language used in each provision identifies their compulsoriness:

Language	What it means	Examples
Shall	Health care facilities must follow these provisions in order to comply with the Standard. These items were designed to be reasonable for HCFs to meet.	4.7.4 *"Workflow mapping... **shall** be completed, identifying where connected systems, devices, and equipment have an impact..."*
Should	These are strong recommendations for health care facilities to follow but are not required. Due to the diversity of health care facilities across the country, these recommendations may not be possible in all situations.	5.2.1.2 *"When determining the data centre, cloud, or data centre and cloud requirements, health care facilities **should** consider the digital health vision and strategy..."*
May	These are options for that which is permissible within the limits of the Standard.	5.4.2.2.2 *"Where necessary, subducts **may** be used when installed inside a conduit..."*

This is a voluntary Standard that HCFs may individually choose to take on, which may eventually be considered for reference in legislation.



What is covered in the standard

Digital health vision and strategy
Requires each HCF to develop a Digital Health Vision, in collaboration with patients, clinical, and non-clinical representatives. Provides a comprehensive framework for Vision creation and describes key features, including a set of guiding principles, governance structures, and more

Future-proofing and lifecycling
Integrates advice throughout about ensuring scalability and agility into digital infrastructure planning

Privacy and security
Directs HCFs to maintain a security and privacy plan and encourages preparing a "security roadmap"

Broader facility planning alignment
Encourages planning for broader infrastructure requirements for digital, including room planning, fire separation, water management, etc.

Asset and tech inventories
Supports HCFs to improve oversight of technology systems and digital tools through ongoing processes and capital projects

Tools for system transformation
Provides tools including costing templates, operational readiness checklists, checklists for device selection, and more

Master Systems Integrator (MSI) role
Highlights the value of an MSI role to act as lead point person on systems integration planning, technology deployment, and interoperability

Catastrophic event planning and redundancy
Requires development of response measures for digital infrastructure, with a focus on providing 100% redundancy for clinical services

Use cases
Offers guidance on developing and deploying use cases to test and plan technologies, and provides 100 example use case scenarios

What is **not** covered in the standard

Electronic health records or medical records
However, complements and supports ongoing work on pan-Canadian health data interoperability

Specific technology solutions for different HCF types
Does not identify particular solutions for HCF types: tech-agnostic and principles-focused

Artificial Intelligence
Does not specifically target Artificial Intelligence or AI implementation in HCFs

Virtual care
Strong digital infrastructure can support vitual care provision but it is not a focus of this Standard

Policy relevance for government

Planning and maintaining high-quality digital infrastructure for health care



***The issue*:** Digital infrastructure is essential to the daily operations of modern hospitals and health care facilities. As health care technology (e.g. devices and platforms) advances, demands on data processing capabilities continue to increase. HCFs require robust and reliable digital infrastructure to securely transmit and store vast amounts of data between specialized equipment, servers, and medical devices. Additionally, infrastructure must incorporate redundancy to prevent isolated component failures from escalating into critical system disruptions.

How the Standard helps HCFs:

The majority of the Standard's text consists of specific, actionable directions on digital infrastructure.

The Standard outlines key directions on such focus areas as:

- Data centres
- Telecommunications pathways and spaces
- Structured cabling
- Network equipment
- Wireless Local Area Networks (WLANs)
- Intrusion detection systems
- Cellular and radio connectivity
- Nurse call systems
- Real-time locating systems
- Wireless staff communication devices

Managing cybersecurity and privacy for health care



The challenge: Health care facilities manage extensive amounts of sensitive personal data, necessitating strong protection against cyber threats and reliable frameworks for privacy. Implementing cybersecurity frameworks strengthens resilience, allowing critical care to continue uninterrupted during incidents. Recent cyberattacks on Canadian hospitals and HCFs have cost millions of dollars, disrupted services, and compromised sensitive information affecting hundreds of thousands of patients.

Although risks to public institutions are well known, Canada's legislative and regulatory environments have not kept pace with evolving cyber threats. Notably, there remains a significant gap in health-care-specific cybersecurity and privacy guidance.

How the Standard helps HCFs:

The Standard provides HCFs with clear steps to strengthen their cybersecurity and privacy practices, enabling them to effectively leverage digital health technologies while proactively managing associated risks.

In alignment with other guidance, the Standard:

- Directs HCFs to establish a privacy and security plan, encompassing threat risk evaluations, privacy impact and vulnerability assessments, and incident response protocols.
- Outlines mandatory components of an effective security incident response plan, including a prioritized list of digital systems and defined maximum allowable downtimes (time without function) per system.
- Requires HCFs to be compliant with the Canadian Centre for Cyber Security's Baseline cyber security controls for small and medium organizations.
- Recommends foundational cyber security training for all HCF staff, covering skills such as secure password practices and identifying malicious emails.
- Requires HCFs to implement procedures for reporting privacy breaches and effectively communicating incidents to interested parties.

Optimizing health care technology coordination and oversight

The challenge: HCFs of all sizes depend on diverse technologies to deliver quality care. Large hospitals may manage hundreds of distinct device types and systems, each varying significantly in lifecycle, function, and compatibility. Often, technology, procurement, and adoption differ by department, driven by their specific needs and immediate cost pressures rather than an integrated approach. This disjointed process can create gaps, leaving HCFs without a clear, comprehensive understanding of their technological landscape and system interactions.



How the Standard helps to support HCFs

The Standard gives structured approaches for HCFs to seamlessly coordinate their technology strategies, offering practical tools for effective procurement, implementation, and change management.

- Requires HCFs procuring new digital health care technologies to:
  - develop business cases in consultation with key interested parties.
  - clearly define roles and responsibilities for technology planning, implementation, and evaluation.
  - identify critical success factors specific to implementation.
  - establish optimal procurement strategies.
- Directs HCFs to assess current and future technological states, including a complete inventory of applications, systems, policies, and contracts necessary to realize their digital health vision and strategy.
- Requires HCFs to develop change management and equipment planning processes to smoothly integrate new technologies.
- Recommends routine reviews of technology inventories in HCFs. Provides practical guidance for testing and validating technology solutions prior to full-scale implementation.

Driving integration, interoperability, and scalability

The challenge: System interoperability failures or network disruptions within HCFs are more than administrative inconveniences – they can directly threaten patient safety. Effective interoperability across systems, equipment, and digital infrastructures is crucial to addressing current challenges and preparing for the future of health care delivery. Enhancing interoperability is also essential for advancing national digital health objectives and achieving pan-Canadian health data mobility. Reliable internal information flow within an HCF is foundational for enabling seamless data exchange across regions and jurisdictions



How the Standard helps to support HCFs

The Standard provides HCFs with clear guidance to incorporate integration and interoperability from the earliest stages of technology planning. It emphasizes developing specific use cases linked directly to clinical and operational outcomes. HCFs can leverage these use cases to rigorously test system integration and overall functionality.

Alongside other direction, this Standard:

- Requires HCFs to create comprehensive integration and interoperability plans aligned with their digital vision and strategy. These plans must consider the role of standards-based and open digital solutions, with clear process and outcome-focused success metrics.
- Requires establishing integration platforms that facilitate effective communication, data exchange, and information translation, thereby supporting robust interoperability.
- Recommends HCFs undergoing digital infrastructure upgrades appoint a dedicated Master Systems Integrator (MSI). This role is responsible for leading system integration deployment plans and coordinating interoperability workflows. The Standard outlines suggested qualifications and key responsibilities for the MSI.

How governments can strengthen digital infrastructure in health care facilities

The rapid integration of digital infrastructure and emerging technologies into health care represents a generational opportunity that demands responsive, agile, and coordinated policy measures.

Standards are particularly valuable in rapidly evolving sectors, as they establish consistent safety and performance practices across Canadian jurisdictions.

Governments already effectively use standards within policymaking frameworks.

While standards are sometimes referenced in legislation and regulation, they are also instrumental in non-legislative contexts, such as strategic planning, procurement processes, program funding designs, and policy guidance. The referencing of CSA Z8005:24 in regulation can significantly enhance security and establish a seamless digital healthcare system. Such a Standard can improve information sharing, streamline healthcare delivery, and ultimately enhance patient care.

CSA Z8005:24 aligns closely with provincial and territorial health care goals,

including sustainability, quality improvement, efficient facility management and design, innovation, and virtual care.

Leveraging CSA Z8005:24 to enhance health care delivery

Technology investments

The Standard highlights the necessity of robust evaluation frameworks, operational readiness, proactive risk management, and continuous improvement processes. These elements help to enable healthcare facilities to effectively assess technology investments, ensuring alignment with efficiency, security, and patient care objectives. Such an approach is vital for breaking down governmental and jurisdictional silos and enhancing interoperability.

Enhanced procurement

Governments can utilize the Standard to move beyond short-term, cost-focused procurement strategies by integrating considerations such as flexibility, scalability, innovation, interoperability, and cybersecurity. This approach helps support lasting, meaningful advancements in Canadian digital health capabilities.

Convening, promotion, and education

Provinces and territories are uniquely positioned to effectively convene their health care leaders, support targeted education initiatives, and foster collaborative commitments to quality improvement and health care performance excellence.

About CSA Group

Canadian Standards Association, operating as CSA Group (CSA), was established over 100 years ago and is Canada's largest accredited standards development organization. We are a member-based association serving business, government, and consumers, with over 3,000 published standards and codes in more than 54 subject areas, including health care, occupational health and safety, the environment, energy, infrastructure, and emerging technologies. Standards developed with our 11,000 members help improve safety, health, the environment, and economic efficiency in Canada and beyond. We collaborate with federal, provincial, and territorial governments to positively impact the lives of Canadians every single day. We believe that governments' support, endorsement, advocacy, and reference of our standards can help deliver a stronger, more sustainable, and resilient Canada.

CSA Group always strives to provide up to date and accurate information. However, no representation or warranty, expressed or implied, is made that this information meets your specific needs and any reliance on this information is at your own risk. Please contact CSA Group for more information about our services.

CSA GROUP™

© 2025 Canadian Standards Association. All Rights Reserved.