A national standard for cybersecurity in healthcare

HealthCare*CAN* and the Digital Governance Council (DGC) with support from Public Safety Canada's Cyber Security Cooperation Program, have jointly published the first national standard on cybersecurity uniquely tailored to the healthcare sector. Entitled *Cybersecurity: Cyber Resiliency in Healthcare,* the standard is the culmination of a three-year project and another tool in HealthCare*CAN*'s efforts to address critical gaps in healthcare cybersecurity.

ADVOCATING FOR GREATER CYBERSECURITY MEASURES

HealthCare*CAN* worked for many years to improve awareness of the need for concerted action and resources to improve cybersecurity and cyber hygiene in healthcare. Since 2017, HealthCare*CAN* has developed policies, recommendations for action, and tools to help hospitals, health authorities, healthcare and health research institutions reduce the risk of cyber threats.

In 2018, HealthCare*CAN* hosted the Canadian Summit for Healthcare Cybersecurity, sponsored by Public Safety Canada's Cyber Security Cooperation Program. The insights and knowledge shared by healthcare leaders from across Canada alongside leading experts in healthcare and cybersecurity from the United Kingdom, France, and the United States at the summit were captured in an Issues Brief and Options Brief to assist Canada's health leaders understand and navigate cybersecurity issues. The event concluded with a set of agreements in-principle to a Declaration of Commitment for Cybersafe Healthcare signed by over two-dozen healthcare organizations from across Canada.

In 2019, HealthCare*CAN* and our member institutions, Eastern Health – the largest integrated health organization in Newfoundland and Labrador, partnered with the Canada-Israel Industrial Research and Development Foundation (CIIRDF) to gather Israeli cybersecurity leaders and Canadian specialists in fields of healthcare, education, information technology, management and private sector partners in a focused discussion on cybersecurity in Canadian healthcare. The partnership led to exploring opportunities to develop new projects in education, software development, and digital infrastructure to support cybersafe healthcare in Canada.

During the pandemic, HealthCare*CAN* supported members by sharing policy briefs highlighting the various opportunities of expanded virtual care as well as the ensuing threats to their IT structure and vaccine development efforts. We regularly attended Canadian Centre for Cyber Security's (CCCS) weekly health sector COVID-19 calls to be aware of cyber threats and share them with our members. We continue to attend the CCCS's bi-weekly threat briefings to stay informed on emerging threats to the healthcare sector.

CURRENT WORK

HealthCare*CAN* represents the health sector on the National Cross-Sector Forum for Critical Infrastructure (NCSF). This multi-sector network is co-chaired by the Deputy Minister of Public Safety Canada and mandated under the National Strategy for Critical Infrastructure to strengthen cross-sector partnerships, share intelligence, and deploy an all-hazards risk management approach to critical infrastructure threats – including cybersecurity threats. As part of our role on this Forum, HealthCare*CAN* works with our partners at the Public Health Agency of Canada to build and maintain a network for health sector critical infrastructure that addresses the sector's needs across domains of critical infrastructure.

HealthCare*CAN* has stressed the need for greater investment in Canadian digital infrastructure to transform the healthcare system to one that has a strong foundation able to support new technology and tools and better share information across institutions and jurisdictions. HealthCare*CAN* has also supported the Government of Canada's Shared Pan-Canadian Interoperability Roadmap by participating in consultations to provide strategic advice.

In our 2024 pre-budget submission to the Standing Committee on Finance, HealthCare*CAN* urged the government to provide a Modernizing Healthcare Infrastructure Fund of $5B, over three years, to improve both physical and digital infrastructure and create a more resilient, sustainable, and equitable health system, and improve patient care and safety.

RANSOMWARE CONTINUES TO BE A THREAT TO HEALTHCARE ORGANIZATIONS

In October, five hospitals in Ontario were attacked with ransomware that caused disruption of essential health services including cancer treatments and surgeries[i]. The hackers released private health information to the dark web after the hospitals refused to pay the ransom. Now, weeks later, the hospitals are still struggling to recover and fully restore services. This is but one of the recent examples of cyberattacks, a threat that will continue to plague hospitals and healthcare facilities, according to the Canadian Centre for Cyber Security[ii].

WHAT CAN THE HOSPITAL SECTOR DO TO SAFEGUARD AGAINST SUCH CYBER THREATS?

Hospitals, health authorities, health research centres, and healthcare organizations can adopt the *Cybersecurity: Cyber Resiliency in Healthcare*, a national standard of Canada, to be better equipped. A standard uniquely tailored to healthcare, it was informed by HealthCare*CAN*'s extensive network of health leaders across Canada and the DGC's (formerly known as the CIO Strategy Council) wide-ranging network of digital and information technology experts.

[i] https://www.cbc.ca/news/canada/windsor/windsor-hospital-ransomware-attack-cybercriminal-group-1.7017176
[ii] https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-impact-covid-19-cyber-threats-health-sector

STANDARD DEVELOPMENT PHASE 1 – FOCUS GROUPS

With support from Public Safety Canada's Cyber Security Cooperation Program, the project to develop the standard began with HealthCare*CAN* and the DGC co-hosting a series of focus groups in English and French with the goal of acquiring feedback from healthcare and health technology leaders on their concerns, issues and needs around cyber security in healthcare. More details on the focus groups and the ensuing results can be found here. The focus groups included over 100 healthcare technology leaders and many other key stakeholders from across Canada. Representation included individuals from hospitals and healthcare organizations, academic and research institutes, national, provincial, and territorial governments, industry, legal professionals, and insurance organizations.

These participants from HealthCare*CAN* and the DGC memberships were asked five key questions:

- What is your biggest area of concern if you become the target of a cyberattack?
- What is the biggest risk to the healthcare system today?
- What focus areas would you like to see included in a National Standard of Canada?
- What are the critical success factors regarding the development and implementation of a national standard for the cybersecurity of Canada's healthcare system?
- Does your organization currently use or is your organization looking to adopt a recognized information/cybersecurity standard?

The feedback from the participants included concerns around patient care, safety, protection of health information, and the ability to ensure continuity of care. Participants also noted that among the major risk factors that needed to be addressed in a healthcare specific standard were ransomware and legacy information technology infrastructure. Participants felt that a tiered approach would ensure accessibility for all organizations and emphasized the need for extensive training for frontline and clinical staff with supporting educational materials.

A draft standard was completed in November 2022, with the guidance from the workshops and the expertise of a Technical Committee as well as an Expert Drafting Team of cybersecurity experts from healthcare organizations, government, and the private sector.

STANDARD DEVELOPMENT PHASE 2 – CONSULTATIONS AND REVIEWS

The Technical Committee held a series of consultations and reviews with representation from health leaders, patients, and caregivers across Canada from January through March 2023. HealthCare*CAN* members provided their feedback on the draft standard both orally and in writing. Some of the key topics emphasized included the important role of leadership in cybersecurity risk management and strengthening cybersecurity awareness, clarifying the role and responsibilities of the leadership team, and the identification and achievement of cybersecurity policies and objectives.

A 60-day public review, with the standard being made available on the DGC's website, began on April 27, 2023, and closed on June 27, 2023. This open opportunity for review provided an additional opportunity for cybersecurity experts, health leaders, and stakeholders across Canada to provide their feedback on the standard. More information on the process and key findings can be found in the peer-reviewed journal article "Enhancing patient safety: A national standard for cyber resiliency in healthcare" published online ahead of the upcoming December edition in Healthcare Management Forum.

KEY RECOMMENDATIONS IN THE STANDARD

The standard incorporates guidelines and best practices that healthcare organizations from hospitals and research institutes to medical clinics and virtual care providers. Addressing a broad range of topics and considerations, from organizational risk management, leadership and education to cyber incident response and contingency planning, the standard provides guidance on how to identify, assess, and manage cyber risks in Canada's healthcare organizations.

The standard stresses the role of senior leadership being responsible for ensuring provision of the resources needed, establishing the cybersecurity policy and objectives and overseeing the organization's cybersecurity program.

Some of the key recommendations for the standard are:

- Developing and implementing an organization-wide information cybersecurity program;
- Documenting and disseminating information security policies and procedures;
- Coordinating the development and implementation of an organization-wide information security training and awareness program;
- Determining and recommending to the leadership team the cyber risk target level of the organization;
- Tracking and providing periodic reports and status updates on the cyber risk target level of the organization;
- Coordinating a response to actual or suspected breaches;
- Identifying organizational risks and prioritizing risk treatment; and
- Delegation of the information security role as required.

In addition, the standard has an incident response plan template, a cyber security risk assessment questionnaire, and other planning templates that will assist users in understanding their current cybersecurity posture and creating a plan tailored for their organization.

NEXT STEPS

The standard is to be revised every five years and will continually evolve to meet the needs of healthcare organizations across Canada. HealthCare*CAN* and the DGC will continue to disseminate key findings and lessons learned from this project with health leaders across Canada and encourage all healthcare organizations and our members to implement the standard. HealthCare*CAN* will also be offering knowledge translation materials in both English and French.

The standard is available here for download free of charge in English and French.

FOR MORE INFORMATION

HealthCare*CAN* remains attentive to our members – if your organization has any questions, feedback in connection with these developments we encourage you to contact us.

Siri Chunduri
Policy and Research Analyst
schunduri@healthcarecan.ca

Jonathan Mitchell
Vice-President, Research and Policy
jmitchell@healthcarecan.ca