REPORT

A Cybersecurity Overview of the Canadian Health Sector

Threats, Solutions and Lessons Learned

Written by: **Louis Melançon** from ***Serene-risc***

August 2020

credit: flaticon

Summary

Introduction

The Canadian health sector is undergoing a slow but irresistible digital transformation. Medical devices that traditionally were standalone are now integrated into hospital networks. Technological innovations in automation and monitoring are improving patient care, especially for acute and chronic conditions[1]. Electronic records allow health professionals to access and share patient information rapidly. Telehealth and virtual care services, already underway before the COVID-19 pandemic, are expected to expand even further. A pan-Canadian electronic health record system allowing for e-prescribing services is being developed by Canada Health Infoway, a not-for-profit tasked with accelerating the country's adoption of digital health solutions[2]. A 2017 survey reported that 32% of Canadian adults use one or more mobile apps to monitor aspects of their health, and 24% own at least one smart device for health and well-being[3].

Although these technological developments bring better care to patients and allow for easier collaboration between healthcare practitioners, they also carry new risks. The benefits of digitalization and interconnectivity are undermined by the new potential harms they can generate. Cybersecurity incidents and data breaches can compromise sensitive data and ultimately endanger care services[4]. Healthcare organizations run on a patchwork of interconnected devices ranging from legacy desktop computers to the latest medical equipment. Constantly changing groups of hospital staff, temporary workers and volunteers interact with this equipment and bring their personal electronic devices to work. This shifting entanglement of users and systems represents a colossal cybersecurity challenge, as devices and individuals which were never meant to interact suddenly come into contact, potentially risking patients' health and exposing sensitive information. According to the World Health Organization, "Information governance—covering areas of privacy, confidentiality, security and informed consent—is becoming a defining issue of our times[5]."

The 2017 *Canadian Survey of Cyber Security and Cybercrime* paints a disturbing picture of current cybersecurity practices in the health sector[6]. Canadian health businesses seem to have been spared so far, as 87% reported not being impacted by any cybersecurity incidents in 2017. However, they also seem woefully unprepared and ill-equipped to face any breach, attack or systems failure:

- 78% of large health organizations and 67% of healthcare businesses overall have only between 1 and 5 employees dedicated to cybersecurity.
- Only 14.6% of healthcare businesses provide cybersecurity-related training to their employees.

[1] Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48-52. LINK
[2] See https://www.infoway-inforoute.ca/en/
[3] Paré, G. et al. (2017). *Diffusion of Smart Devices for Health in Canada*, CEFRIO, Montreal, Quebec, Canada, 55 pp. LINK
[4] Stinson, C. (2018). *Healthy Data: Policy Solutions for Big Data and AI Innovation in Health*. Mowat Centre for Policy Innovation. LINK
[5] https://www.who.int/ehealth/programmes/governance/en/
[6] See https://www150.statcan.gc.ca/n1/pub/71-607-x/71-607-x2018007-eng.htm

- Only 51.5% reported monitoring their network and systems.

The WannaCry ransomware attacks of spring 2017 were a watershed moment in demonstrating the concrete dangers of cybersecurity incidents for healthcare organizations. Exploiting a known but widely unpatched vulnerability in Microsoft Windows, the malware spread and encrypted systems' files, locking out users until they made a ransom payment. The attack affected more than 200,000 computers in at least 100 countries, but it had a particularly severe impact in the United Kingdom, where 80 out of 236 National Health Service trusts were directly affected[7]. Thousands of appointments and operations were canceled as hospitals and clinics were either infected or had turned off their systems as a precaution. Ambulances carrying trauma patients had to be diverted from affected institutions, risking lives. Despite being notified of the dangerous system vulnerability several weeks in advance of the May outbreak, a significant number of NHS trusts were still running an unpatched or unsupported version of the Windows operating system. Ransomware attacks have continued to affect healthcare organizations since, including in Canada. Three Ontario hospitals were targeted in September 2019. In the case of the Michael Garron Hospital, the malware spread from a single corporate laptop to infect most systems, including electronic medical records, taking ten days to restore access[8]. In September of 2020, a ransomware attack in Düsseldorf, Germany forced a hospital transfer that directly resulted in the death of a patient[9].

Ransomware attacks are severe but represent only a small portion of the potential cyber threats facing health organizations. Researcher Sarah Lewis of the Open Privacy Research Society discovered in November 2018 that sensitive medical information of patients admitted to certain Vancouver hospitals was being broadcast unencrypted by hospital paging systems. Patients' names, age, gender, diagnosis, attending doctor and room number could be trivially intercepted by anyone in the Greater Vancouver Area. Vancouver Coastal Health reacted months after the researcher's private disclosure, after Lewis contacted journalists and the breach appeared in the news. The hospital network consequently affirmed it believed patient data was protected, and had been unaware of the radio broadcasting component of their pager system[10]. Asset management of technological equipment is another difficult challenge healthcare organizations are currently facing, among many others.

Cyber Threats to Healthcare

Any discussion of cybersecurity within the healthcare environment must stem from the principle that healthcare security is a patient safety issue[11]. Cybersecurity has historically been viewed in the healthcare industry as a problem confined to Information Technology departments. Incidents are

[7] Morse, A. (2018). Investigation: WannaCry cyber attack and the NHS. *Report by the National Audit Office*. LINK
[8] Owens, B. (2020). How hospitals can protect themselves from cyber attack. *CMAJ*. LINK
[9] Tidy, J. (2020) Police launch homicide inquiry after German hospital hack. *BBC News*. LINK
[10] https://openprivacy.ca/blog/2019/09/09/open-privacy-discovers-vancouver-patient-medical-data-breach/
[11] Thompson, C. (2018). *Moving Forward for Cybersafe Healthcare*. HealthCareCAN. LINK

approached reactively rather than proactively and are considered detached from patient care[12]. As the WannaCry attacks have demonstrated, data breaches and cyber attacks can have direct and dire consequences for health services. Cybersecurity incidents affect a lot more than data alone.

Healthcare organizations are prime targets for cyberattacks and data breaches. They represent a unique sector in terms of the breadth and depth of the information they collect and store[13]. In addition to the sensitive health data of their patients, health organizations also may possess financial information such as credit card numbers and bank accounts, business intelligence and intellectual property such as medical research, as well as national security information related to emergency procedures. The combination of highly vulnerable systems, significant financial resources and potentially life-threatening consequences for patients makes medical providers an especially attractive target for malicious attackers.

The *Health Industry Cybersecurity Practices* report[14], published in 2018 for the US Department of Health & Human Services by a task group of more than 150 healthcare and cybersecurity experts, identified these five cybersecurity threats as the most prevalent and impactful for the health sector:

- **Email Phishing Attacks**: Phishing is a type of internet fraud in which malicious actors trick victims into unknowingly disclosing sensitive information. Victims are typically lured to a fraudulent website impersonating a well-known brand where they are prompted to enter personal data. Email is a major vector for phishing and malware infection.
- **Ransomware Attacks**: Ransomware is a type of malicious software that threatens to perpetually block access to or publicly release victims' data until a ransom is paid. In some instances, such as the WannaCry attacks, the malware automatically spreads to other computers without user interaction. Interestingly, the very first ransomware attack in 1989 targeted medical researchers[15].
- **Loss or Theft of Equipment or Data**: Mobile devices such as laptops, tablets, smartphones and USB drives used in a healthcare environment may contain highly sensitive information. Lost or stolen on the premises or outside the organization's walls, these devices may result in the unauthorized access and dissemination of private information if not appropriately safeguarded.
- **Insider, Accidental or Intentional Data Loss**: Employees, contractors and other users of a health organization's systems may access or disseminate sensitive information, either accidentally or intentionally. An employee could be tricked into divulging private information or could accidentally leak important data. That employee could also deliberately access sensitive information to use it for personal gain.
- **Attacks Against Connected Medical Devices That May Affect Patient Safety**: Disruptions affecting any device used for the diagnosis, treatment or prevention of a medical condition

[12] HCIC Task Force (2017). *Report on Improving Cybersecurity in the Health Care Industry*. LINK
[13] Vesely, R. (2019). *The Board's Role in Cybersecurity (Part One)*. American Hospital Association. LINK
[14] US Department of Health and Human Services (2018). *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*. LINK
[15] https://www.beckershospitalreview.com/healthcare-information-technology/first-known-ransomware-attack-in-1989-also-targeted-healthcare.html

could severely impact patient care. Given the large size and interconnectedness of medical equipment networks, such devices are highly vulnerable.

In the context of the global COVID-19 pandemic, cybercriminals are taking advantage of the situation to conduct their malicious activities. As health organizations increasingly rely on remote work solutions, gateway appliances and virtual private networks are actively targeted by criminals and state-sponsored actors. Although the Canadian Center for Cyber Security has not yet been engaged in providing assistance related to an attack against a Canadian hospital, healthcare centers in the Czech Republic, United States, Spain and Germany were targeted by ransomware attacks between March and April 2020[16].

Security Measures

Healthcare has an open, sharing culture which, while appropriate to its primary mission, complicates information security considerations[17]. Large teams of health practitioners, from different departments or even different organizations, need access to the data of their thousands of patients quickly and easily. Healthcare personnel may, for instance, leave workstations unlocked and unattended in order to expedite collaboration with their colleagues. Until the recent news of cyberattacks around the world affecting healthcare, security professionals had difficulty convincing health organizations of the very real dangers they were facing. The harmful reality of practices sacrificing the security of computers systems for the sake of ease or efficiency has been laid bare. The Canadian health sector needs to adapt its work culture to minimize cybersecurity risks. Everybody, from board members to practitioners and equipment manufacturers, needs to raise the priority of cybersecurity through proactive and consistent measures.

Public Safety Canada, in its *Fundamentals of Cyber Security for Canada's CI Community* report, recommends four major safeguards which "would prevent the vast majority of exploits" for any critical infrastructure[18]:

- **Application whitelisting**: Limiting what software can be executed on a computer system according to a curated list of pre-approved applications protects devices and their networks against potentially harmful applications.
- **Use modern operating systems and applications**: Using modern and actively maintained applications ensures that they benefit from the latest security protections and fixes. Organizations should establish a life-cycle approach to migrate to newer versions.

[16] Canadian Centre for Cyber Security (June 2020). *Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threats to the Health Sector*. LINK
[17] HCIC Task Force (2017). *Report on Improving Cybersecurity in the Health Care Industry*. LINK
[18] Public Safety Canada (2016). Fundamentals of Cyber Security for Canada's CI Community. LINK

- **Patch operating systems and applications**: Patching within a two-day timeframe of a high-risk vulnerability being made public ensures that computer systems and their networks are protected as soon as possible from potential attackers exploiting the vulnerability.
- **Restrict administrative privileges**: Minimizing the number of users with a domain or local administrative access to a system or device prevents equipment misconfiguration and limits the potential damage resulting from a cyberattack.

The US *Health Industry Cybersecurity Practices* report provides further recommendations in line with its assessment of cyber threats that are tailored to health organizations[19]. Cybersecurity measures and their scope must correspond to an organization's scale and resources.

1. **Email protection systems**: Email is commonly leveraged for credential theft and malware infection attacks. Organizations should properly configure their email servers, antispam and antivirus filtering controls, as well as provide workforce education.
2. **Endpoint protection systems**: Endpoints are the desktops, laptops, workstations and mobile devices used to interface with an organization's digital ecosystem. Organizations should adopt full disk encryption, limited usage of administrator accounts as well as rigorous provisioning practices.
3. **Identity and access management**: Properly granting, revoking and managing user access enables the right individuals to access the right resources at the right time. Organizations should establish clear procedures for access provisioning, transfer and revocation as well as implement large and complex passwords for privileged accounts
4. **Data protection and loss prevention**: Healthcare organizations must thoroughly understand where their data resides, how it is used and how it is transmitted within and outside their networks. They should classify information according to sensitivity levels, data encryption practices and backup strategies.
5. **IT Asset Management**: Information technology assets should be rigorously managed for the complete duration of their life-cycle: procurement, deployment, maintenance and decommissioning. Organizations should maintain a complete inventory listing and establish procurement and decommissioning procedures.
6. **Network management**: Networks are the core infrastructure allowing communications and equipment interoperability. Organizations should deploy firewalls, network segmentation practices such as providing a guest network for visitors and ensure the physical security of network devices.
7. **Vulnerability management**: Proactively scanning systems for vulnerabilities allows organizations to prioritize threats, mitigate vulnerabilities and prevent attacks. Organizations should assess risks and exposure relative to measures 4 to 6, patch their systems rapidly and implement penetration testing.
8. **Security operations center and incident response**: Not all attacks can be prevented, and accidents do happen. It is important to develop the capability to detect incidents and

[19] See the report's appendix titled *Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations* for the full and detailed list of security practices LINK

respond quickly when they happen. Organizations should establish clear remediation efforts guidelines, detailed responsibilities and information sharing protocols.

9. **Medical device security**: Because of their highly regulated nature, of the special skill required to modify them and their life-critical quality, traditional security measures cannot necessarily be deployed on medical devices. Organizations should establish proper and potentially different access, asset, network and vulnerability management according to manufacturer guidelines. **Making configuration changes or applying a security patch to a medical device without direct approval from the manufacturer is ill-advised and dangerous.**
10. **Cybersecurity policies**: Policies should make clear to the workforce of health organizations how and why they are expected to behave with regard to cybersecurity. Organizations should clearly define roles and responsibilities, establish acceptable email practices, official guidelines for personal device use at work as well as define an incident reporting checklist.

Implementing cybersecurity measures in a healthcare setting is very difficult. Security is mostly intangible until an incident arises. Risks are difficult to assess in advance, and cybersecurity is never guaranteed, which makes it difficult to fund and defend in front of executive boards[20]. Many medical professionals see cybersecurity standards as an impediment to their work and patient care in general[21]. Security measures can for instance decrease the time they can spend with patients and potentially reduce the ease of collaboration among staff. Jalali and Kaiser, in their 2018 study of the dynamics of cybersecurity capabilities development in US hospitals, have identified its two most effective strategies, neither of which entail pursuing more resources. The two priorities of chief information and security officers, according to their research, should be to **reduce endpoint complexity** and to **improve internal stakeholder alignment**[22]. As equipment systems and networks become larger and more interconnected, complexity increases, and cybersecurity capabilities correspondingly erode at an increasing speed. Moving to cloud-hosted services and maintaining stricter policies on technology procurement are two suggested measures to reduce endpoint complexity. Decision-making is similarly complex within health organizations. Issues are debated between the board of directors, executives, IT and bioengineering staff, as well as care workers. Security professionals interviewed by Jalali and Kaiser claimed that medical staff are the hardest to convince related to cybersecurity measures. These experts suggested that 1) experiencing a cyber crisis, 2) having security issues articulated in terms of patient harm and 3) designing systems with unobtrusive security measures are the three keys to success in convincing cybersecurity skeptics[23].

[20] de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1-7. LINK

[21] Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: a systematic, organizational perspective. *Journal of medical Internet research*, *20*(5), e10059. LINK

[22] *Ibid.*

[23] *Ibid.*

Canadian Regulation

Canadian privacy laws are integral to the healthcare cybersecurity landscape since they regulate how institutions can collect, use and disclose patient information, one of their most critical assets. There are two federal privacy laws, enforced by the Office of the Privacy Commissioner of Canada[24]:

- The **Privacy Act**[25], which covers how the federal government handles personal information;
- the Personal Information Protection and Electronic Documents Act[26] (**PIPEDA**), which covers how businesses handle personal information.

PIPEDA establishes how private-sector organizations can collect, use and disclose personal information in the course of for-profit activities in Canada. Organizations covered by PIPEDA must generally obtain an individual's consent when they collect, use or disclose that individual's personal information. People have the right to access their personal information held by such an organization or to challenge its accuracy. PIPEDA includes a list of ten principles organizations are required to follow: accountability; identifying purposes; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access and challenging compliance. PIPEDA does not apply to organizations that do not engage in commercial, for-profit activities, or to Alberta, British Columbia and Quebec, which have general private-sector laws that have been deemed substantially similar to PIPEDA[27].

The following provincial acts define the additional responsibilities that health information custodians bear in their handling of health data. They have been declared substantially similar to PIPEDA with respect to health information:

- Ontario's Personal Health Information Protection Act[28] (**PHIPA**);
- New Brunswick's Personal Health Information Privacy and Access Act[29] (**PHIPAA**);
- Newfoundland and Labrador's Personal Health Information Act[30] (**PHIA**);
- Nova Scotia's Personal Health Information Act[31] (**PHIA**).

[24] https://www.priv.gc.ca/en/
[25] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/
[26] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
[27] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/
[28] https://www.ipc.on.ca/health-individuals/file-a-health-privacy-complaint/your-health-privacy-rights-in-ontario/
[29] https://www2.gnb.ca/content/gnb/en/departments/health/privacy_and_access.html
[30] https://www.gov.nl.ca/hcs/phia/
[31] https://novascotia.ca/dhw/phia/

In some borderline cases, such as health data generated by wearable technology, businesses working with hospitals on health technology or hospitals collaborating across provincial borders, it can be difficult to tell which jurisdiction is responsible[32].

On November 1, 2018, Canadian businesses became subject to new mandatory breach reporting regulations under PIPEDA. Whereas data breach reporting was formerly done on a voluntary basis, organizations subject to PIPEDA are now required to report to the Privacy Commissioner Office any breaches of security safeguards involving personal information. The Commissioner's office reported receiving 680 breach reports between November 2018 and October 2019, which is six times the volume they had received during the same period one year earlier[33]. Efforts are currently underway to modernize privacy laws both on the federal and provincial level. A major revision of the federal Privacy Act, introduced in 1983, has been in discussion for many years[34]. Quebec's Bill 64, introduced in June 2020, similarly aims to modernize the province's protections for personal information. If adopted, Bill 64 would introduce "privacy by design" requirements, mandatory breach reporting, updated consent requirements and increased penalties for noncompliance, with fines up to $25 million[35].

Conclusion

The WannaCry attacks of 2017 and the many incidents which have continued to happen worldwide since have finally drawn the attention of governments and healthcare providers towards better cybersecurity practices. Organizations that have been directly impacted by these attacks and breaches have typically implemented new security measures, which other health providers can learn from.

The United Kingdom's National Health Service has identified many lessons to learn from WannaCry, including the need to:

- Develop a detailed response plan with clearly defined roles for local and government entities;
- Ensure organizations implement critical recommendations by government cybersecurity entities, including promptly applying software patches and keeping antivirus software up to date;

[32] Stinson, C. (2018). *Healthy Data: Policy Solutions for Big Data and AI Innovation in Health*. Mowat Centre for Policy Innovation. LINK
[33] Privacy Commissioner of Canada (2019). *A full year of mandatory data breach reporting: What we've learned and what businesses need to know*. LINK
[34] https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html
[35] Tehrani, M. et al. (2020). *Quebec to Introduce the Most Punitive Privacy Laws in Canada—With Fines of up to $25 Million*. Gowling WLG. LINK

- Ensure essential communications can get through when systems are down, via alternative channels;
- Ensure that everybody from the executive board to patient care staff understands the direct risks to front-line services and takes the necessary proactive measures[36].

Closer to us in Ontario, the Michael Garron Hospital, which was affected by a ransomware attack in September 2019, announced it now keeps a list of staff cellphone numbers to use during future emergency shutdowns. Realizing that younger staff had difficulties reverting to using paper charts and documentation during downtime, they also implemented a specialized training program[37]. This corresponds to Zhao et al.'s conclusions following their study of the impact of a ransomware attack's downtime on residency training in a US hospital[38]. They reported that residents, accustomed to having constant online access to health information and having not worked before the digitalization of hospital systems, were caught off guard and significantly stressed. The authors recommend that medical education includes preparedness for cybersecurity threats, similar to what already exists for other disasters such as natural catastrophes and infectious outbreaks.

Although technological innovations bring better care to patients and allow for easier collaboration between healthcare practitioners, they also carry new risks. Cybersecurity incidents and data breaches can compromise sensitive data and ultimately endanger care services. Canadian health businesses, although they seem to have been mostly spared so far, unfortunately seem unprepared to face breaches and attacks according to the latest surveys. The Wannacry ransomware attacks of spring 2017 have been followed by many more such attacks around the world, including in Canada, which continue to this day. Email is an especially potent vector of phishing and malware infection, often at the source of system breaches. After ransomware, other major cybersecurity threats for health organizations include loss or theft of equipment, insider data loss and attacks against connected medical devices.

Healthcare has an open, sharing culture which can complicate security considerations. Health professionals will consider cybersecurity measures as an impediment to their work if they interfere with patient care. Studies have suggested that 1) reducing endpoint complexity and 2) improving internal stakeholder alignment were the two most effective strategies in improving cybersecurity capabilities development in health organizations. Designing systems with unobtrusive security measures and articulating security issues in terms of potential harm to patients are key in communicating security norms to medical personnel.

[36] Morse, A. (2018). Investigation: WannaCry cyber attack and the NHS. *Report by the National Audit Office*. LINK
[37] Owens, B. (2020). How hospitals can protect themselves from cyber attack. *CMAJ*. LINK
[38] Zhao, J. Y. et al. (2018). Impact of trauma hospital ransomware attack on surgical residency training. *Journal of surgical research*, *232*, 389-397. LINK

Aditional Resources

For additional resources and recommendations on cybersecurity best practices, health organizations and their practitioners can consult the Serene-risc website[39] as well as the Global Cyber Alliance's Cybersecurity Toolkit for small to medium-sized businesses[40]. Helpful resources there include:

- A hardware and software asset tracking spreadsheet to facilitate asset management;
- Templates for USB device use and software patching company policies;
- Password management tools and recommendations;
- Links to website security scanning tests

[39] https://www.serene-risc.ca/en/cybersecurity-tips
[40] https://gcatoolkit.org/smallbusiness/