UPDATED VERSION, Nov. 27, 2023

Analysis CPD

Cyberattacks on Canadian health information systems

Vinyas Harish BCompH, Alun Ackery MD MSc, Kiran Grant MD, Trevor Jamieson MD MBI, Shaun Mehta MD GPLLM

■ Cite as: *CMAJ* 2023 November 20;195:E1548-54. doi: 10.1503/cmaj.230436

Canadian health systems have digitized considerably. In 2019, 86% of surveyed Canadian family physicians reported using electronic medical records (EMRs).[1] Digital tools for virtual care and remote patient monitoring, wearables, care coordination platforms, and Internet-of-things (IoT) devices are all permeating practice.[2] The digitization and integration of disparate health information systems on shared networks promises greater convenience, access and quality of care, but also introduces risk for patients, providers and health systems. Although some clinicians have dedicated information technology (IT) training, most do not, and navigating increasingly complex health information systems can create considerable stress.

Cyberattacks can incur privacy breaches and financial harm, as well as compromise patient safety and health system functioning. Personal health information (PHI) can fetch much higher prices on the dark Web than other personal information (e.g., credit card details).[3] In a 2021 international survey of health IT decision-makers, the average cost of a ransomware attack was US$1.27 million.[4] Cyberattacks against health information systems have been associated with delays in care, diversion of patients to other sites and increased mortality.[5] Cyberattacks against Canadian health information systems are increasingly common, with 48% of all reported 2019 Canadian breaches occurring in the health sector.[6] Cyberattacks have also been increasing amid events such as the COVID-19 pandemic and Russo–Ukrainian War.[7,8] We outline the impact of cyberattacks on Canadian health information systems and how clinicians, whether they practise in large hospitals or individual clinics, can improve their cybersecurity posture.

Key points

- Cyberattacks can incur privacy breaches and financial harm, as well as directly threaten patient safety and health system functioning.
- Reducing the risk of cyberattacks and managing those that do occur happens in 4 stages: prevention, detection, response and recovery.
- As novel areas of cyberthreats emerge (e.g., Internet-connected devices), clinicians and health organizations should be vigilant for recalls, keep software up to date and discuss possible risks with patients.
- Keeping workflows efficient and maintaining a strong cybersecurity posture has trade-offs; however, the minor inconveniences of security measures such as 2-factor authentication are far preferable to recovering from an attack.

How have cyberattacks affected Canadian health information systems?

Cyberattacks against health information systems are most commonly ransomware or data breaches (Figure 1). At least 14 major cyberattacks on Canadian health information systems have occurred since 2015, 9 of which attempted ransom and 6 of which compromised PHI. Ransomware involves the installation and activation of a malicious program (i.e., malware) that locks or encrypts a computer system and its stored data until a financial ransom is paid. Access to data is commonly lost even when ransoms are paid.[4] The attack can also entail data breaches, whereby PHI is exfiltrated off health information systems and shared illicitly in online marketplaces. Another form of extortion relies on denial of service, whereby an attacker overwhelms a site through fake traffic to make it unavailable for authentic users (e.g., patients attempting to book an appointment) until a payment is made.[9] Although most cyberattacks against health organizations are attributed to criminals, they can also be perpetrated by nation-states, terrorist groups, online "hacktivists" and ideologically motivated violent extremists (e.g., those targeting abortion centres).[10–12]

Health organizations, irrespective of their size, make attractive cyberattack targets. First, they are financially lucrative targets because of the value of PHI but are also likely well-resourced enough to pay ransoms. Since attackers adjust ransom amounts to the perceived ability of the target to pay, attackers can hold health information systems in individual physician offices for ransom in the Can$3000–Can$5000 range and still expect a reasonable likelihood of payment.[13] Canadian hospitals have not been reported to pay ransoms, but American health systems have paid ransoms well into the millions of dollars.[14] Even if no money is paid, the extortion attempt can still incur extended periods of downtime of the health information system with substantial (and very public) impacts to IT and patient services. Second, the extensive media coverage of cyberattacks on health systems increases the pressure on victims

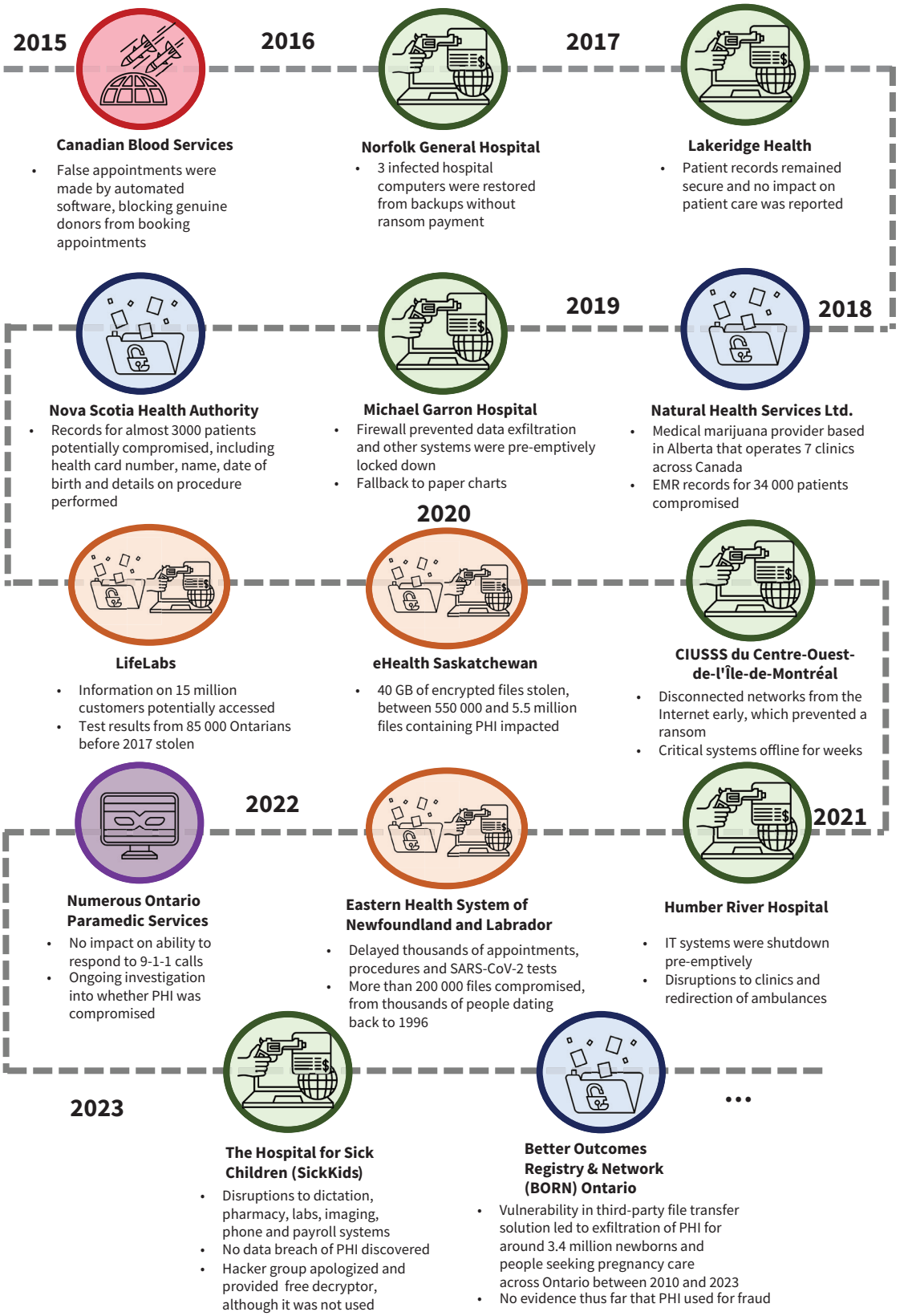

Figure 1: Recent cyberattacks on Canadian health information systems, including denial of service (red), ransomware (green), data breach (blue), mixed (orange) and unknown (purple). Note: IT = information technology, PHI = personal health information.

to pay the ransom quickly before it becomes public. Third, health organizations often have a history of underinvesting in IT systems and rely on outdated or legacy systems that are vulnerable to exploitation. Finally, health organizations can also lack the capacity to respond to cyberthreats, which increases the damage of hacks as well as the probability of paying ransoms.

What can Canada learn from the cybersecurity practices of peer countries?

Comprehensive comparison of the burden of attacks between jurisdictions is difficult since many cyberattacks on health information systems are unreported.[15] Although effective cyberhygiene (i.e., daily routines, good behaviours and occasional check-ups akin to principles in health) strategies for end-users are essentially universal across organizations, sectors and jurisdictions, cybersecurity policy in Canadian health information systems has considerable room for improvement.

In June 2022, the House of Commons proposed the *Critical Cyber Systems Protection Act* (CCSPA). The CCSPA defines critical cyber systems as those with serious implications for public safety if compromised. These systems include telecommunications, pipelines, nuclear energy, federally regulated transportation and banking — but not health organizations.[16] In contrast, the United States Cybersecurity and Infrastructure Security Agency supports a range of Sector Coordinating Councils that collaborate with the government for information sharing, coordination and the establishment of voluntary practices to promote resilience. The Healthcare and Public Health Sector Coordinating Council has dozens of members, including health systems, advocacy groups, insurers and nonprofit organizations.[17] Although the exclusion of health organizations from the CCSPA could be viewed as consistent with the federal–provincial principles of the *Canada Health Act*, governance mechanisms such as Sector Coordinating Councils could promote adherence to common standards while also fostering innovation and experimentation.

Within the provinces and territories, considerable heterogeneity exists in cybersecurity posture among broader public sector organizations, as smaller institutions often lack requisite financial and human resources. Shared services models can help address disparities. For example, Ontario Health is piloting 6 regional security operation centres.[18] Each centre would continuously monitor the security practices of member institutions, defend against breaches and proactively isolate and mitigate security risks. Regional security operation centres are similar to the well-received, health-related computer emergency response teams in the United Kingdom, Norway and the Netherlands.[10] As governments establish these bodies, clinicians and health organizations must develop familiarity with them and their incident reporting and escalation pathways. During establishment of these bodies, governments should also endeavour to engage clinicians to ensure their needs and perspectives are considered. Provinces and territories should be wary of regulating cybersecurity practices beyond reporting at the level of the individual provider or health organization (e.g., mandating biannual cybersecurity audits) as top–down requirements can be overly onerous in terms of effort, capital and human resources, especially for smaller practices. Finally, provinces and territories should establish publicly available repositories of cyberattacks on health information systems.[15] Such repositories can serve as a useful aid for research and guide consumer choice as patients may preferentially seek out providers with strong cybersecurity track records.

How can clinicians prevent and navigate cyberattacks?

The US National Institute of Standards and Technology outlines 5 stages to effectively navigating cyberattacks: identification, protection, detection, response and recovery.[19] For simplicity, we have combined the stages of identification and protection into a single prevention stage (Figure 2).

Prevention

At the individual level, cyberhygiene prevents attacks. Clinicians should be vigilant for phishing attacks via email or other suspicious behaviour (Figure 3). Phishing refers to targeted, deceptive efforts to gain access to a victim's device or network. Once access has been obtained, an attacker can install malware to exfiltrate or encrypt data for ransom. Clinicians should ensure they use unique, strong passwords (i.e., at least 8 characters with a mix of letters, numbers and special characters) and 2-factor authentication for their logins, as well as set up verification questions and auto-lock devices with access to PHI. Password managers can generate and store unique, strong passwords for each site and provide notifications when user information is compromised. Clinicians should avoid sensitive tasks without adequate network protections (e.g., accessing patient records on public Wi-Fi) as data can be intercepted or malware can be installed in "man-in-the-middle" attacks. Software must be kept up to date as developers release patches for security vulnerabilities on an ongoing basis. Health organizations are notorious for relying on legacy systems (e.g., Windows XP) well past the date of their security support deprecation.

At the institution or practice level, a key aspect of preventing cyberattacks is to reduce the attack surface, or the number of entry points an intruder would have into health information systems. This is especially important with setups in which individuals can use their personal devices and with increasing numbers of IoT devices.[20] Techniques for reducing attack surfaces include auditing all devices on the network, ensuring that their software (including operating systems) are up to date, installing antivirus and antimalware software, and setting up a firewall to monitor both outbound and inbound Internet traffic. Practices can also set up a virtual private network (VPN), which encrypts and disguises online traffic, making it much more difficult to intercept. Virtual private networks are particularly important for clinicians who wish to access PHI from environments outside their health organization's network, such as to complete charting at home. Although clinicians in larger organizational settings will have the benefits of a standardized approach, those in private practice will have to rely on third-party vendors. Luckily, many traditional antivirus vendors now have comprehensive bundles of services. Professional support from organizations such as the Ontario Medical Association exists, including privacy

Cyber-safety practices for Canadian physicians

How physicians, clinics and hospitals can mitigate the risk of a cybersecurity attack

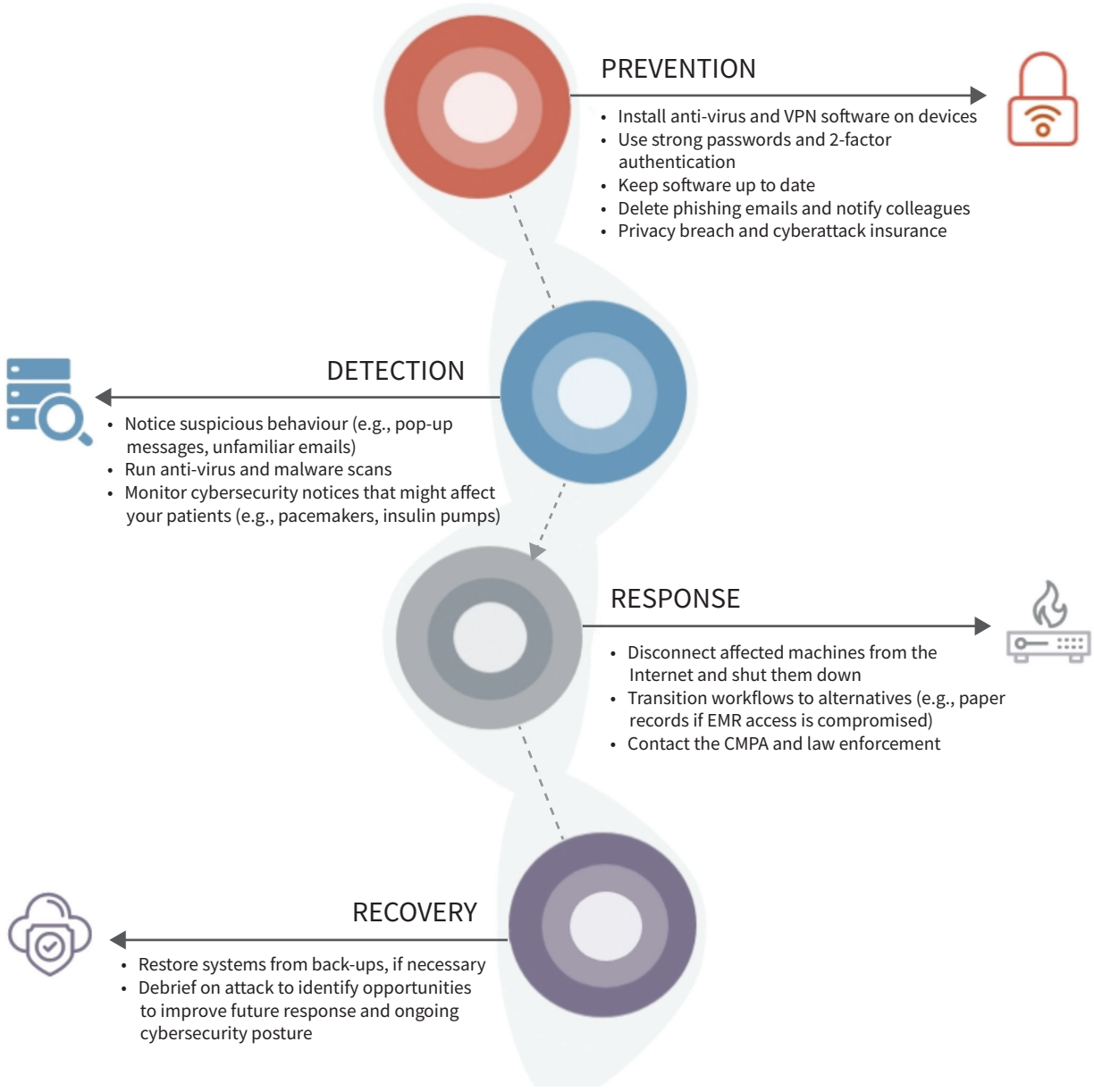

Figure 2: Four stages of cyber resilience, with suggested actions. Note: CMPA = Canadian Medical Protective Association, EMR = electronic medical record, VPN = virtual private network.

breach and cyber coverage to assist with forensics, public relations and legal services. These should be viewed as essential office expenses and, in many jurisdictions, may be eligible for tax credits.

Detection

Suspicious behaviour can indicate a cyberattack. Examples include barred entry to files or applications (e.g., EMRs, email clients), the deletion or installation of unrecognized files and software, program auto-running and emails sent without the user's consent. Ransomware attacks are often accompanied by pop-up messages that indicate to the user that they are being hacked and that provide instructions and a deadline for ransom payment. Antivirus or antimalware software can also detect threats on routine scans. Finally, users within the organization may report that they followed a link in a phishing email or downloaded unknown files or applications.

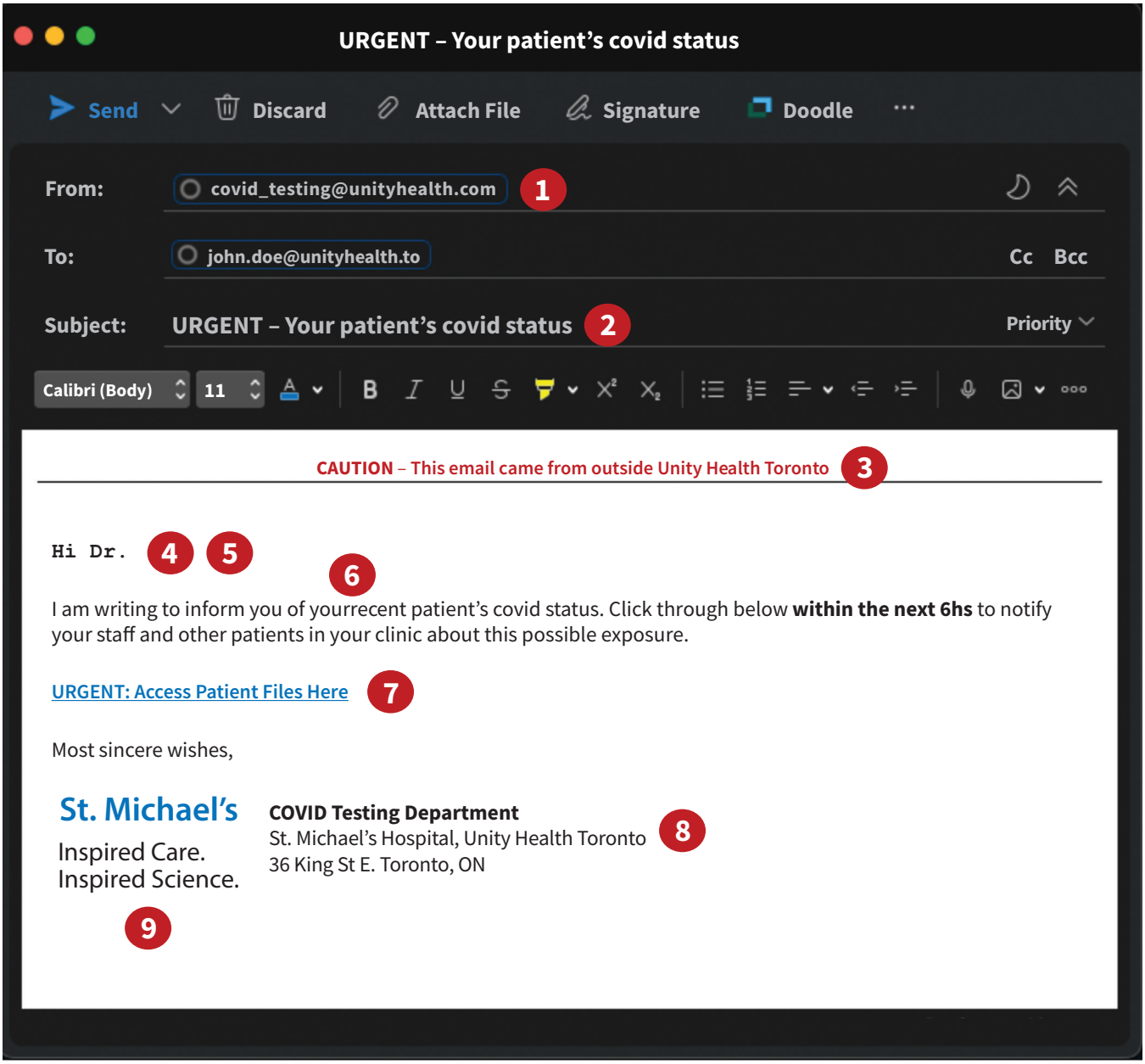

Figure 3: Anatomy of a hypothetical phishing attack.

Response

Once a cyberattack is detected, clinicians should first disconnect affected machines from the Internet and shut them down. Quick action can prevent the exfiltration of data, including PHI, from a health organization's device and network. Once this is done, practices should activate their cyberattack response plan. If access to computerized systems such as EMRs is lost, staff should transition to back-up workflows such as using paper records. Depending on the magnitude of workflow disruptions and the ability of clinicians to maintain an adequate standard of care, contingency measures such as cancelling clinics and transferring patients may be needed. Crucially, response plans should not be improvised but rather be well

documented, clear and deliberately practised.[21] Clinicians should practise their cyberattack response (i.e., their code grey) like they would a fire (i.e., their code red). Although the pressure to do so may be immense, health organizations should generally not pay ransoms to unlock and decrypt systems, because restored access is not guaranteed and paying ransoms may encourage future attacks.

The Canadian Medical Protective Association (CMPA) outlines the duty of custodians to notify affected individuals of privacy breaches (e.g., patients), as well as the provincial or territorial privacy commissioner and ministry of health.[22] As the nuances of expectations vary across jurisdictions, the CMPA recommends organizations and clinicians initiate contact with the CMPA as soon as possible after a possible breach is discovered. They should also contact law enforcement, especially in the event of a ransomware attack. The Royal Canadian Mounted Police is currently pilot-testing a National Cybercrime and Fraud Reporting System.[23] The Canadian Centre for Cyber Security also has a reporting system; however, it does not trigger an immediate response by law enforcement.[24] As part of their cyber response plan, practices should consult relevant authorities in advance to ensure they clearly understand the obligations for breach reporting and notification of law enforcement for their jurisdiction.

Recovery

After the acute threat of a cyberattack has subsided, clinicians and their organization can then enter the recovery phase. Recovery is heavily dependent on having health information systems that allow for restoration from back-ups. For smaller organizations and independent practices without dedicated IT experts, clinicians should ask how their vendors will protect their data and help recover it in case of an attack as part of their due diligence when making a purchase. Organizations should also have a focused debrief on the response, with emphasis on opportunities for improvement and measures to improve ongoing cybersecurity posture.

Clinicians may feel that adhering to the outlined actions only adds to the burden imposed on them by health information systems. In his famous *The New Yorker* essay, Atul Gawande quipped that the EMR systems "that promised to increase my mastery over my work [have], instead, increased my work's mastery over me."[25] Especially for clinicians in smaller practices, cybersecurity can become another dimension of task load, in addition to documentation, computerized order entry and maintenance of licensing requirements through mandatory e-modules, all of which contribute to burnout.[26,27] Simulation training has also become commonplace in medicine and some may ask if more are necessary. Measures such as 2-factor authentication and VPNs add complexity to workflows; however, small changes to daily practices that promote cyberhygiene are far preferable to recovering from a cyberattack operationally, both financially and in terms of patient and community trust.

What are emerging areas of cybersecurity in health care?

Emerging technologies require attention to ensure that the risk of compromise does not grow with improvements in utility. Clinicians who are adopting a virtual care platform should note that consumer video-conferencing solutions (e.g., Zoom, FaceTime) often do not meet provincial privacy and security requirements. Instead, clinicians should use tools built into their EMR or versions of videoconferencing solutions that specifically meet health care standards such as Zoom for Healthcare.[28] Provincial health authorities provide lists of verified solutions for virtual care.[29] Personal medical devices — such as pacemakers, insulin pumps and blood glucose monitors — are connected to the Internet for remote biomarker monitoring, as well as to receive software updates. Hackers have shown the ability to rapidly drain device batteries, provide too much stimulus (e.g., pacing, insulin bolus) or fail to provide a stimulus when clinically indicated.[30] In 2019, Health Canada recalled several models of insulin pumps that were susceptible to attack and encouraged patients to discuss switching to other models with their physicians.[31] Finally, machine learning tools are actively being developed and integrated into health care workflows.[32] These tools can be vulnerable to adversarial attacks or subtle changes to input data that are carefully designed to mislead algorithms toward incorrect outputs.[33] For example, a hacker can add very small amounts of noise to pixels in a radiograph that would be imperceptible to humans but change model outputs (e.g., from benign to pathologic or vice versa). Across these novel areas, clinicians and health organizations should be vigilant for recalls, keep software up to date and discuss possible risks with patients.

Conclusion

Preventing cyberattacks involves navigating trade-offs between keeping workflows efficient and reducing risk amid threats that are growing in frequency, severity and sophistication. As national and regional policies develop, health organizations, practices and individual clinicians must take a proactive approach to improving their cybersecurity posture. Methods for handling personal and professional risk go hand-in-hand, including leveraging tools and best practices, being vigilant and having an incident response plan. With respect to cybersecurity, a bit of prevention is worth a terabyte of cure.

References

1. *How Canada Compares: Results from the Commonwealth Fund's 2019 international Health Policy Survey of Primary Care Physicians*. Ottawa: Canadian Institute for Health Information; 2020:1-78. Available: https://www.cihi.ca/sites/default/files/document/cmwf-2019-accessible-report-en-web.pdf (accessed 2023 Oct. 29).
2. Cohen AB, Dorsey ER, Mathews SC, et al. A digital health industry cohort across the health continuum. *NPJ Digit Med* 2020;3:68.
3. HC3 intelligence briefing update dark web PHI marketplace: overall classification is unclassified. Washington (DC): The U.S. Department of Health & Human Services; 2019:1-13. Available: https://content.govdelivery.com/attachments/USDHSFACIR/2019/04/25/file_attachments/1199378/Dark%20Web%20primer.pdf (accessed 2023 Oct. 29).
4. The state of ransomware in healthcare 2021. Abingdon (UK): SOPHOS; 2021:1-16. Available: https://assets.sophos.com/X24WTUEQ/at/s49k3zrbsj8x9hwbm9nkhzxh/sophos-state-of-ransomware-in-healthcare-2021-wp.pdf (accessed 2023 Oct. 29).
5. *The impact of ransomware on healthcare during COVID-19 and beyond*. Traverse City (MI): Ponemon Institute; 2021. Available: https://www.censinet.com/wp-content/uploads/2021/09/Ponemon-Research-Report-The-Impact-of-Ransomware-on-Healthcare-During-COVID-19-and-Beyond-sept2021-1.pdf (accessed 2023 Oct. 29). Login required to access content.

6. Burke D. Hospitals 'overwhelmed' by cyberattacks fuelled by booming black market. *CBC News* 2020 June 2. Available: https://www.cbc.ca/news/canada/nova-scotia/hospitals-health-care-cybersecurity-federal-government-funding-1.5493422 (accessed 2023 Oct. 29).
7. Alert: Cyber threats to Canadian health organizations. Canadian Centre for Cybersecurity; 2020. Available: https://www.cyber.gc.ca/en/alerts-advisories/cyber-threats-canadian-health-organizations (accessed 2023 Oct. 29).
8. Samarasekera U. Cyber risks to Ukrainian and other health systems. *Lancet Digit Health* 2022;4:e297-8.
9. Nigrin DJ. When 'hacktivists' target your hospital. *N Engl J Med* 2014;371:393-5.
10. Wilner AS, Luce H, Ouellet E, et al. From public health to cyber hygiene: cybersecurity and Canada's healthcare sector. *Int J* 2021;76:522-43.
11. Vinall F. Huge Australian health hack exposes abortion patients and others. *The Washington Post* 2022 Nov. 10, updated 2022 Nov. 11; Available: https://www.washingtonpost.com/world/2022/11/10/australia-health-data-hack-abortion/ (accessed 2023 Sept. 9).
12. Schaffer A, Marks J, Knowles H. Planned parenthood Los Angeles says hack breached about 400,000 patients' information. *The Washington Post* 2021 Dec. 1; Available: https://www.washingtonpost.com/nation/2021/12/01/los-angeles-planned-parenthood-hack/ (accessed 2023 Sept. 9).
13. Taggart K. The hacker in the clinic: why physicians have become targets of ransomware attacks and what you should know. *The Medical Post*; 2019;32-4. Available: https://www.ontariomd.ca/articlesdocumentlibrary/hacker_in_the_clinic_med_post_oct_2019.pdf (accessed 2023 Oct. 29).
14. Landi H. UCSF pays hackers $1.1M to regain access to medical school servers. New York: Fierce Healthcare; 2020. Available: https://www.fiercehealthcare.com/tech/ucsf-pays-hackers-1-14m-to-regain-access-to-medical-school-servers (accessed 2023 Oct. 29).
15. Neprash HT, McGlave CC, Cross DA, et al. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021. *JAMA Health Forum* 2022;3:e224873.
16. Ahmad I, Cassell J, Corovic T, et al. Bill C-26: the increased importance of Canadian cybersecurity. Ottawa: Norton Rose Fulbright Insights. 2022. Available: https://www.nortonrosefulbright.com/en-ca/knowledge/publications/42944ded/bill-c26-the-increased-importance-of-canadian-cybersecurity (accessed 2023 Oct. 29).
17. Healthcare and public health sector: council charters membership. Arlington (VA): US Cybersecurity & Infrastructure Security Agency. Available: https://www.cisa.gov/healthcare-and-public-health-sector-council-charters-membership (accessed 2023 Oct. 29).
18. Jones P. How to deter cyber-attacks: TOH outlines its best practices. Thornhill (ON): Canadian Healthcare Technology; 2022. Available: https://www.canhealth.com/2022/09/01/how-to-deter-cyber-attacks-toh-outlines-its-best-practices/ (accessed 2023 Oct. 29).
19. Cybersecurity Framework (CSF). Gaithersburg (MD): National Institute of Standards and Technology; 2016, updated 2023 Aug. 15. Available: https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters (accessed 2023 Sept. 9).
20. Alexandrou A, Chen L-C. Perceived security of BYOD devices in medical institutions. *Int J Med Inform* 2022;168:104882. doi: 10.1016/j.ijmedinf.2022.104882.
21. Report a cyber incident. Canadian Centre for Cyber Security; modified 2022 Feb. 21. Available: https://www.cyber.gc.ca/en/incident-management (accessed 2023 Sept. 9).
22. Willing M, Dresen C, Gerlitz E, et al. Behavioral responses to a cyber attack in a hospital environment. *Sci Rep* 2021;11:19352.
23. Reporting a privacy breach: What are your responsibilities? Ottawa: Canadian Medical Protective Association; 2018, revised September 2022. Available: https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2018/the-new-reality-of-reporting-a-privacy-breach (accessed 2023 Oct. 29).
24. New cybercrime and fraud reporting system. Ottawa: Royal Canadian Mounted Police; modified 2021 Sept. 23. Available: https://www.rcmp-grc.gc.ca/en/new-cybercrime-and-fraud-reporting-system (accessed 2023 Sept. 9).
25. Gawande A. Why doctors hate their computers. *The New Yorker* 2018 Nov. 5; Available: https://www.newyorker.com/magazine/2018/11/12/why-doctors-hate-their-computers (accessed 2023 Sept. 20).
26. Sinsky C, Colligan L, Li L, et al. Allocation of physician time in ambulatory practice: a time and motion study in 4 specialties. *Ann Intern Med* 2016;165:753-60.
27. Hodzic-Santor B, Prakash V, Raudanskis A, et al. How many hours do internal medicine residents at University of Toronto spend onboarding at hospitals each year? A cross-sectional survey study. *medRxiv* 2022 June 14. doi: 10.1101/2022.06.10.22276103.
28. Appendix 2: Best practices security for Zoom virtual health visits. Vancouver: Provincial Health Services Authority; updated 2020 June 2. Available: http://www.phsa.ca/health-professionals-site/Documents/Office%20of%20Virtual%20Health/Security%20best%20practices.pdf (accessed 2023 Oct. 29).
29. Verified solutions list for virtual visits. Toronto: Ontario Health. Available: https://www.ontariohealth.ca/system-planning/digital-standards/virtual-visits-verification/verified-solutions-list (accessed 2023 Oct. 29).
30. Baranchuk A, Refaat MM, Patton KK, et al.; American College of Cardiology's Electrophysiology Section Leadership. Cybersecurity for cardiac implantable electronic devices: What should you know? *J Am Coll Cardiol* 2018;71:1284-8.
31. Certain older Medtronic MiniMed insulin pumps may be vulnerable to cybersecurity risks [public advisory]. Ottawa: Government of Canada, Health Canada, Communications and Public Affairs Branch; modified 2019 June 29. Available: https://recalls-rappels.canada.ca/en/alert-recall/certain-older-medtronic-minimed-insulin-pumps-may-be-vulnerable-cybersecurity-risks (accessed 2023 Oct. 29).
32. Verma AA, Murray J, Greiner R, et al. Implementing machine learning in medicine. *CMAJ* 2021;193:E1351-7.
33. Finlayson SG, Bowers JD, Ito J, et al. Adversarial attacks on medical machine learning. *Science* 2019;363:1287-9.

Competing interests: Alun Ackery is provincial medical director with CritiCall Ontario. No other competing interests were declared.

This article has been peer reviewed.

Affiliations: Temerty Faculty of Medicine (Harish), University of Toronto; Institute of Health Policy, Management, and Evaluation (Harish), Dalla Lana School of Public Health, University of Toronto; Department of Emergency Medicine (Ackery, Mehta), St. Michael's Hospital, Unity Health Toronto, Toronto, Ont.; Department of Emergency Medicine (Grant), Faculty of Medicine, University of British Columbia, Vancouver, BC; Department of General Internal Medicine (Jamieson), St. Michael's Hospital, Unity Health Toronto; Institute for Health System Solutions and Virtual Care (Jamieson), Women's College Hospital; Department of Emergency Medicine (Mehta), North York General Hospital, Toronto, Ont.

Contributors: All of the authors contributed to the conception and design of the work, drafted the manuscript, revised it critically for important intellectual content, gave final approval of the version to be published and agreed to be accountable for all aspects of the work.

Funding: Vinyas Harish was supported by the Canadian Institutes of Health Research Banting and Best Canada Graduate Scholarship (Doctoral) and the Schwartz Reisman Institute for Technology and Society Graduate Fellowship.

Correspondence to: Vinyas Harish, v.harish@mail.utoronto.ca