Securing Public Trust in Digital Healthcare

Resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombudspersons with Responsibility for Privacy Oversight

Context

1. Canada's health sector continues to experience serious resource constraints and staff shortages, aggravated by more than two years of surges in demand for emergency care brought on by the ongoing COVID-19 pandemic.

2. These and other complex problems facing the health sector during the pandemic have spurred innovation and change in the delivery of services, including through virtual care visits and other forms of digital health communications.

3. However, despite these rapid digital advancements in the health sector, breaches continue to be caused by the use of insecure communication technologies such as traditional fax[1] machines and unencrypted emails, unauthorized access to health records by employees (often in the form of 'snooping'), and cybersecurity attacks (including ransomware).

4. Personal health information is one of the most sensitive types of information about an individual. Data breaches in the health sector can cause significant harm to affected individuals, including potential discrimination, stigmatization, financial and psychological distress.

5. If individuals begin to lose trust in the health system, they may withhold or falsify personal health information, avoid treatment, or hesitate to consult their health providers altogether -- putting their own lives and health at risk in order to protect their privacy.

6. Furthermore, breaches can consume an inordinate amount of time and effort to contain and remediate, taking away valuable health resources from other important services. Misdirected communications and data breaches can also create delays in the delivery of care to individuals, cause harm to institutions' reputations, and set back public trust in the health system.

7. Privacy is not a barrier to innovation. Ensuring that the shift to digital healthcare is secured by reasonable administrative, technical and physical safeguards is critical to maintaining Canadians' trust in the health system. Furthermore, the adoption of secure digital technologies can provide relief from the administrative, financial and reputational costs associated with privacy breaches.

8. Many groups across Canada have recognized the inherent value of privacy-protective digital health innovations. For example, the Expert Advisory Group for a Pan-Canadian Health Data Strategy recently issued its final report where they recommended the adoption of a Canadian Health Data Charter that, among other things, calls for "security and privacy of health data to maximize benefit and reduce harm."

9. There are now numerous modern and practical alternative ways to facilitate the legal and secure sharing of personal health information, when and as necessary to deliver health

[1] Traditional fax" refers to facsimiles (faxes) that require a paper copy of a record of personal health information to be scanned through a fax machine then transmitted via a telephone line to a recipient fax machine that prints the scanned transmission onto paper to re-create the original copy.

services. Examples of these include encrypted email services, secure patient portals, electronic referrals, and electronic prescribing.

10. These alternatives, when properly configured with built-in privacy protections and a user-centric design, can be made more auditable, secure, and resilient against unauthorized access or inadvertent disclosure.

11. Such digital technologies are already being successfully integrated into digital medical record systems such as electronic medical records (EMRs), electronic health records (EHRs) and hospital information systems (HIS).[2]

12. To protect and bolster public trust in digital healthcare, action must be taken across Canadian jurisdictions to modernize and protect communications involving personal health information in step with the expanding array of digital means now available to better secure the sharing and use of this highly sensitive information.

THEREFORE

13. Canada's Privacy Commissioners and Ombudspersons with responsibility for privacy oversight across the country call on governments, health sector institutions and health providers to show concerted effort, leadership, and resolve in implementing modern, secure and interoperable digital health communication infrastructure. More specifically, we collectively urge the following stakeholders to:

Federal/Provincial/Territorial Governments

14. Develop a strategic plan and provide appropriate supports, funding or other incentives to phase out the use of traditional fax and unencrypted email and replace them with more modern, secure and interoperable digital alternatives in a coordinated fashion;

15. Ensure that all digital health information sharing infrastructure, including solutions that replace traditional fax and unencrypted email, are equitably available and accessible to all Canadians, including those living in remote areas, among marginalized communities, and within vulnerable populations;

16. Promote the adoption of secure digital technologies and the implementation of responsible data governance frameworks that provide reasonable protection of personal health information against unauthorized access or inadvertent disclosures; and

17. Amend laws and regulations, as necessary, to further provide for meaningful penalties, including administrative penalties where appropriate, for health institutions and providers that do not take reasonable measures necessary to protect personal health information as well as for individuals who unlawfully collect, use, or disclose personal health information.

---

[2] EHRs are often regarded as secure and interoperable records of your health history that are accessible across a number of health care institutions and providers. EMRs are electronic patient record keeping systems typically constrained to a specific primary care physician or group of primary care physicians. HIS are, similarly, electronic patient record keeping systems typically constrained to a specific hospital.

Health Sector Institutions and Providers

18. Phase out the use of traditional fax and unencrypted email, as soon as reasonably possible, for communicating personal health information and replace them with modern, secure, and interoperable ways of transmitting personal health information such as encrypted email services, secure patient portals, electronic referrals and electronic prescribing;

19. Design, adopt and implement responsible data governance frameworks, including the adoption of standards such as those developed by ISO, NIST, or CIS that provide reasonable safeguards to protect personal health information, including constant monitoring of electronic systems, periodic audits of all sources of risks to privacy and security, and effective incident response plans and mitigation measures in the event of breach;

20. In the process of modernizing means of communicating personal health information and before procurement, seek guidance from relevant experts to understand how to evaluate new digital health solutions;

21. When evaluating digital health solutions, assess their compatibility with other digital assets, compliance with health information privacy laws, and how they facilitate the rights of individuals to access their own records of personal health information;

22. Promote transparency by completing privacy impact assessments and proactively publishing a plain-language summary in a manner that is easily accessible to the public; and

23. Use the procurement process to help ensure third-party compliance by establishing contractual requirements for vendors of health information software and services.

Furthermore, Canada's Privacy Commissioners and Ombudspersons with responsibility for privacy oversight will work collaboratively in committing to:

24. Collaborate with governments, regulatory colleges, health sector and other relevant stakeholders to provide privacy and security guidance as the health sector transitions toward modern, secure and interoperable digital alternatives for communicating personal health information;

25. Educate individuals about the risks and opportunities associated with digital communications and virtual health care services, their rights to privacy and confidentiality in respect of their personal health information and how they may exercise those rights and hold others accountable;

26. Provide privacy and security guidance to relevant stakeholders on how to fulfill their obligations and preserve public trust;

27. To the extent our respective laws permit, take joint or collaborative enforcement action, as appropriate to address systemic practices in the health sector that are unreasonable because they create unacceptable and easily avoidable risks to the privacy and security of personal health information.