UNIVERSITY OF ALBERTA

Health Law Institute
Faculty of Law, Law Centre, University of Alberta
89 Avenue and 111 Street, Edmonton, AB, T6G 2H5

Fast Facts: privacy considerations in the Canadian regulation of commercially-operated healthcare artificial intelligence

Blake Murdoch[i,ii], Allison Jandura[i] and Timothy Caulfield[i]
[i] Health Law Institute, Faculty of Law, University of Alberta, Edmonton, Alberta, Canada
[ii] Corresponding author: bmurdoch@ualberta.ca

Artificial intelligence (AI) are increasingly being developed and implemented in healthcare. This presents privacy issues since many AI are privately owned and rely on public-private partnerships and data sharing arrangements that use patient health information. We investigated the Canadian legal and policy framework focusing on two issues: first, the potential for inappropriate treatment, use or disclosure of personal health information by private AI companies, and second, the potential for privacy breaches that use newly developed AI methods to reidentify patient health information. Some of our key findings and recommendations are summarized below.

- Patients have a general right to informed consent for the use and disclosure of their personal health information and have an ongoing control interest which necessitates the need for recontact for new uses or disclosures. Public-private partnerships implementing healthcare AI should prioritize the ability to recontact patients.
- The scope of data made accessible to private AI companies should be based on respect of patients' informed consent and rights of ongoing control over their private information. Also, it should be proportional to the likelihood and meaningfulness of the potential benefits the AI can provide.
- Patients have a general right of withdrawal from participation in healthcare AI. AI companies will need to plan for how to respect this.
- Domestic third parties that are transferred patient heath information should have greater legal responsibility to protect it.
- Penalties levied against AI companies for breach of privacy requirements should in our view not be fixed or limited in any way that could fail to deter breaches.
- The concept of "non-identifiable information" is increasingly questionable or even dubious. The subsection of health information that could arguably meet this standard is decreasing quickly over time. Regulators and policymakers must incorporate into their work the reality that technical methods of breaching privacy are quickly improving.
- Access to patient data must be predicated on maintaining highly advanced forms of data security, and anonymization where possible. Strong privacy protection will be required in light of advancing technology that allows data to be re-identified and misused.
- The issue of data security is shared among both institutions that grant access to patient data for AI companies to use, and the AI companies manipulating or storing patient data themselves. Responsibility for security must be shared.
- Enforcement of very high standards for data protection will be key. Governments should consider creating interdisciplinary task forces focused specifically on creating, refining and implementing technical standards for protecting patient health information.