CANADIAN PRIVACY LEGISLATION AND THE CROSS-BORDER TRANSFER OF PERSONAL INFORMATION

PART ONE: PERSONAL HEALTH INFORMATION

By: Candice Teitlebaum & Aaron Collins

An Electronic Health Record (EHR) is the health record of an individual that is accessible online from many separate, interoperable automated systems within an electronic network.[1] An EHR Infostructure is a collection of technical services that allow EHRs to be accessed and updated by authorized healthcare providers, regardless of where the patient and healthcare providers are geographically located within Canada.

EHR Infostructure proponents claim that this system offers tremendous opportunities to deal with the modern challenges of the Canadian health system. The potential advantages include improved quality, timeliness, accessibility and efficiency of health care provided to individual patients and within the healthcare sector as a whole.[2] Initiatives such as the EHR Infostructure are indicative of the general shift toward the electronic storage of data that is taking place in many industries and sectors across Canada. While this shift will undoubtedly lead to greater efficiency and accessibility, such a widely accessible system that stores the personal health information of Canadians also has tremendous privacy implications if appropriate information governance guidelines are not established.

Within Canada, the protection of personal health information is regulated by various federal and provincial privacy laws which establish standards for health information governance and patient privacy rights.[3] The *Personal Information Protection and Electronic Documents Act* (PIPEDA)[4] applies to both federal and provincial entities in the course of conducting commercial activities. Accordingly, PIPEDA applies to information collected, used or disclosed in the course of commercial activities in the health sector, including private pharmacies, laboratories and healthcare providers in private practices.[5] In addition, Ontario has enacted the *Personal Health Information Protection Act* (PHIPA),[6] which contains provisions specific to health information and contains specific rules relevant to health records.

One issue that concerns Canadians generally and health information custodians specifically is transborder data flows to the United States and the existence of the USA PATRIOT Act.[7] While the data contained in an EHR may be collected in Canada, the seamless movement of information across borders facilitates the disclosure of such information outside of Canada. Data

---

[1] Canada Health Infoway Inc., White Paper on Information Governance of the Interoperable Electronic Health Record (EHR), March 2007 [hereinafter White Paper].
[2] *Ibid.*
[3] *Ibid.* at 26.
[4] S.C. 2000, c.5.
[5] White Paper at 27.
[6] S.O. 2004, c.3.
[7] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001,* U.S. H.R. 3162, S. 1510, Public Law 107-56 [hereinafter USA PATRIOT Act].

collected for an EHR may be transferred outside of a Canadian jurisdiction for numerous purposes – for processing, for long-term storage, ancillary to a commercial transaction involving health services, or for patient treatment outside of the jurisdiction.

Both PIPEDA and PHIPA contain specific provisions which can be employed to protect health information stored in Canada. However, if personal health information is transferred outside of Canada by a government agency or a private organization, the laws of the country to which the information has been transferred will apply.[8] This is particularly disconcerting given the reality that while many custodians of EHRs store such records in Canada, a significant amount of the personal information of Canadians is stored in information banks which are located in the United States.

The USA PATRIOT Act, which was enacted in 2001 as a response to the events of September 11, 2001, expanded the power of U.S. law enforcement officials to obtain personal information records stored within the United States. For example, the USA PATRIOT Act permits U.S. law enforcement officials, for the purpose of an anti-terrorism investigation, to seek a court order that allows access to the personal records of any person without that person's knowledge, as long as the relevant records are stored in the United States. This affords U.S. law enforcement authorities power to gain access to Canadian personal information in records held by a U.S.-linked firm, including a Canadian company operating in the United States. Accordingly, it is vital that attempts are made to ensure that data included in the interoperable EHR, and electronic health records generally, remain under Canadian jurisdictional control when contracts are negotiated with EHR service providers and companies are solicited for the purpose of storing personal health information.

Investigations by the Ontario Information and Privacy Commissioner (IPC) highlight the need to ensure that EHRs and personal health information remain in Canada to avoid the compelled disclosure of personal information pursuant to statutes such as the USA PATRIOT Act. On March 10, 2005, the IPC issued a decision regarding a complaint under PHIPA.[9] The complainant had read a news release indicating that a hospital would be working with a U.S. company to develop a strategy for creating an EHR Infostructure. The complainant was concerned that U.S. officials might seek to access the information under the USA PATRIOT Act. The hospital in question explained that it was a pilot program in the conceptual design stage, and if it were made operational, personal health information would not leave the Province of Ontario. The IPC and complainant agreed that due to this explanation there was no basis for proceeding with the complaint. Nonetheless, the fact that the complaint arose in the first place is indicative of the sensitive privacy issues that one must consider when developing a system to process and store personal health information.

More recently, the IPC conducted an investigation into Initiate™ Software, which is used in the Ontario index that stores data relating to individuals for laboratories, hospitals, clinics and the

[8] Office of the Privacy Commissioner of Canada, "Transferring Personal Information about Canadians Across Borders – Implications of the USA PATRIOT Act," August 18, 2004.
[9] See IPC Decision HC-050004-1, March 10, 2005.

Ministry of Health and Long-Term Care.[10] The investigation arose as a result of a news article detailing the investment of In-Q-Tel (the Central Intelligence Agency's investment arm) in Initiate™ Software. The IPC determined that due to very stringent controls, In-Q-Tel did not have access to any personal health information. These controls included: i) contractual provisions in service agreements specifying permitted uses of the information; ii) prohibiting remote access to, or the removal of, personal health information; iii) requiring secure storage of the information in Ontario; iv) requiring consent from any party before disclosure is made; and v) notification requirements should Initiate™ Software be required to breach the service agreement by disclosing personal health information, including circumstances whereby certain legislation, such as the USA PATRIOT Act, compel personal information collection and disclosure. The IPC's decision regarding Initiate™ Software demonstrates that the involvement of U.S. companies in the collection, processing or storage of EHRs will not necessarily pose a problem pursuant to PHIPA, provided adequate contractual controls are established.

The IPC's findings in the Initiate™ Software report echo the general trend of privacy legislation compliance under PIPEDA, PHIPA and other similar statutes across Canada. The general trend is to allow bodies, both public and private, to use mechanisms like the EHR Infostructure to realize efficiency gains and increased accessibility, provided proper governance guidelines are in place. The movement to more outsourcing of data processing and storage means that a large component of proper governance guidelines for health care providers will deal with transborder data flows to the United States, or any jurisdiction with legislation similar to the USA PATRIOT Act.

The key focus for health care providers in Ontario is to ensure that all service agreements contain contractual provisions to provide equivalent protection of personal information that has been transferred outside of Canada. By setting out specific controls pertaining to access to personal information, the service agreements should describe where the personal information will be stored, establish safeguards to ensure information will not be inappropriately disclosed, and develop a procedure to be adhered to in the event that privacy breaches do occur. Essentially, the contractual provisions should indicate that any third party to whom personal health information is disclosed must maintain safeguards to protect the relevant personal health information. Third parties must also protect against unauthorized usage, modification, copying, accessing or other unauthorized processing of such data. In this regard, the objective is to ensure the security and confidentiality of all records and data, protect against anticipated threats or hazards to the security or integrity of information, and protect against unauthorized access to or use of information. The sufficiency of these controls will invariably depend on the specific language used when drafting such service agreements.

Part Two of this article will focus on employee data and employment-related information. For more information on this topic, or any other legal topic relating to corporate, privacy or technology law, please do not hesitate to contact Candice Teitlebaum at 416.865.4743 or cteitlebaum@airdberlis.com.

Candice Teitlebaum is an associate at Aird & Berlis LLP and belongs to the Corporate/Commercial Group and Technology Industry Team. Aaron Collins is a Student-at-Law at Aird & Berlis LLP.

---

[10] See "Investigation Report - PHIPA Report HI06-45 Initiate Systems Inc. and the Ontario Ministry of Health and Long-Term Care," http://www.ipc.on.ca/images/Findings/up-phipa_hi06_45_rpt.pdf.