Canadian Personal Data Protection Legislation and Electronic Health Records: Transfers of Personal Health Information in IT Outsourcing Agreements

Dara Lambie[*]

INTRODUCTION

There is an inevitable tension between the promotion of societal benefits that arise from the free-flow of information, and the protection of individual privacy and personal data.[1] This is so in any sector, but both elements of the dichotomy are heightened when the context is the healthcare sector and the information in question is personal health information. There is a distinct interest in having accurate, readily accessible information available to health professionals because the lives and physical well-being of patients are at stake. Timely access to an individual's health history could mean the difference between life and death. To this end, there has been a great deal of interest in establishing a national electronic health record ("EHR") by which health information could be easily shared by health practitioners. However, there is also a keen concern in protecting, limiting and constraining the disclosure of that same data since information regarding health is among the most sensitive information available about an individual. Unauthorized disclosure of the fact that an individual has, for example, a mental health condition or a potentially stigmatizing disease such as HIV can have serious negative social, professional and economic consequences for the individual.

Personal data protection and privacy of personal health information in the electronic era is a broad topic that includes consent, security measures and access considerations. The focus of this article is on one component of the larger picture: data transfers of personal health information that occur in the context of information technology ("IT") outsourcing. If the societal good envisioned by an inter-ju-

---

* Dara Lambie is an articling student at Blake, Cassels and Graydon LLP in Toronto. Thanks to Elizabeth McNaughton and Margaret Wilkinson and anonymous peer reviewers for their helpful comments.

1 This tension can be seen clearly in one of the earliest articulations of personal data protection; The Organization for Economic Co-Operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD, 1981) [OECD Guidelines]. The dual purpose of the OECD guidelines is to protect the "fundamental human right" of privacy inherent in personal data, and to promote the cross-border flow of information. It was recognized that the two concepts were interlinked and that the latter is potentially at odds with the former. See also Office of the Privacy Commissioner of Canada, *Processing Personal Data Across Borders Guidelines* (Ottawa: Office of the Privacy Commissioner of Canada, 2009) at 4 [PIPEDA Guidelines].

risdictional EHR is to be fully realized, then the necessity of outsourcing is a reality that must be addressed.

I. THE ELECTRONIC HEALTH RECORD

The Office of the Health and Information Highway of Health Canada has defined an EHR as "a health record of an individual that is accessible online, from many separate, interoperable automated systems within an electronic network."[2] Canada Health Infoway, the non-profit corporation established by the federal government to help realize a pan-Canadian EHR, describes it as "a secure, digital record of [an individual's] medical history, stored and shared via a network of EHR systems."[3] The essential element of an EHR is that it is an electronic record that contains personal health information collected over a period of time (an individual's life) that can be accessed by a health professional. An EHR is a network that can be accessed or amended by different health care providers, at different times and in different locations, and is not a single database.[4]

The goal of a coordinated, national electronic health information network is principally to promote enhanced patient care by ensuring that information about the patient is complete, accurate, current and readily accessible.[5] This is especially critical in emergency situations where decisions must be made quickly and often without the benefit of input from the patient himself or herself. Proponents also cite increased efficiencies when data is readily available to a number of care providers. Time and resources are saved when care of a patient is transferred from one individual or organization to another, if the whole of a patient's history does not have to be orally or manually conveyed. This kind of administrative simplification has the potential to significantly reduce the global costs of providing healthcare. While this monetary benefit may be secondary to the importance of timely and appropriate care of the individual, the broader social good cannot be ignored.[6]

Historically, the development of a nation-wide, coordinated EHR has been an official government objective. The federal and provincial governments have pro-

---

2 Office of the Health and Information Highway, Health Canada, *Toward Electronic Health Records* (Ottawa: Office of the Health and Information Highway, 2001) at 9.

3 Canada Health Infoway, online: About Electronic Health Records <http://www.infoway-inforoute.ca/lang-en/about-ehr>. See also Canada Health Infoway Inc., *White Paper on Information Governance of the Interoperable Electronic Health Record (EHR)*, March 2007.

4 See Anthony A. Morris, "The Electronic Health Record in Canada: The First Steps" (2005) 14:2 Health Law Review 14.

5 *Ibid.* at 14; Nola M. Ries & Geoff Moysa, "Legal Protections of Electronic Health Records: Issues of Consent and Security" (2005) 14:1 Health Law Review 18; Lawrence Gostin, "Health Information Privacy" (1994) 80 Cornell L. Rev 451 at 455-456.

6 Indeed, in Gostin, *ibid.*, the emphasis of the tension is between an *individual's* interests in privacy of health records and the *public* or *societal* good, while other commentators have highlighted the tension as between two competing interests of private individuals; individual patient care being paramount over more general societal benefits. See Ries & Moysa, *ibid.*; Morris, *supra* note 4; Glenn Griener, "Electronic Health Records as a Threat to Privacy" (2005) 14.1 Health Law Review 14.

vided much of the impetus and funding for a coordinated network. However, digitalization of health records by individuals and organizations for their own purposes and general record keeping was, and is, inevitable. The practices of individual organizations, outside of direct government initiatives, to create an EHR raise many of the same issues of privacy and data protection. Laws that deal with personal data protection of health information apply to EHRs and this is probably where they will come to light most often in the future given the complex nature, vast amounts of data, and multitude of players in such health infrastructure systems. However, personal data protection legislation also applies to organizations that hold personal health information that is not a part of a patient care network and to non-electronic records, to the extent that they continue to exist. The following discussion will consider both of these scenarios, although they are unarguably interconnected.

II. PERSONAL DATA PROTECTION LEGISLATION OVERVIEW

Personal data protection legislation is enacted at both federal and provincial levels and applies to both public and private sector organizations. All of the acts apply, in varying ways, the principles articulated in the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[7] developed and propagated by the Organization for Economic Co-Operation and Development. These guidelines cover issues such as the collection of data, quality maintenance, security safeguards and a right of individuals to access their own information. For the purposes of this analysis, primary consideration is given to the provisions that regulate the use and disclosure of information since these are applicable to IT outsourcing arrangements. A "use" refers to the kinds of things companies do with information to accomplish their own objectives and meet their own needs. "Disclosure" occurs when information is transferred to another organization that will make use of the information for other purposes unrelated to those of the original organization.

Federally, the *Privacy Act*,[8] the earliest of personal data protection legislation enacted in Canada, regulates the federal public sector. Each province also has personal data protection legislation that applies to provincial government organizations. The *Personal Information and Electronic Documents Act*, ("PIPEDA")[9] regulates the private sector. PIPEDA applies not only to the federally regulated private sector, but also includes the provincial private sector, although it provides that certain classes of organizations and activities may be exempt from PIPEDA if there is provincial legislation that applies to that organization or activity and is substantially similar to PIPEDA.[10] Currently, Alberta,[11] British Columbia[12] and Quebec[13] have

7 OECD Guidelines, *supra* note 1.

8 R.S.C. 1985, c. P-21.

9 S.C. 2000, c. 5.

10 *Ibid.,* section 26(2)(b).

11 *Personal Information Protection Act*, S.A. 2003, c. P-6.5.

12 S.B.C. 2003, ch. 63.

13 *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q. c. P-39.1.

provincial private sector personal data protection legislation that has been declared substantially similar to PIPEDA.

In Ontario,[14] Alberta,[15] Manitoba,[16] and Saskatchewan[17] there is personal data protection legislation that is specific to the health sector. It applies to certain designated public and private bodies that collect, use and disclose personal health information. In Ontario, the *Personal Health Information Act* has been declared substantially similar to PIPEDA and so replaces it in the designated health sector with respect to information held in Ontario. In the other provinces, the health legislation has not been declared substantially similar so the applicable private and public sector personal data protection laws that apply in addition to health-sector-specific laws. In provinces where there is no health-specific personal data protection legislation, health information is governed by the applicable public and private sector data protection legislation.

In this paper, the discussion of IT outsourcing and information transfer within that context will focus on three jurisdictions within Canada: British Columbia, Ontario and the federal PIPEDA as it applies in provinces without substantially similar legislation and to information transferred across jurisdictional borders. There are both historical and conceptual reasons for these choices. British Columbia was the first place in Canada where the cross-jurisdictional flow of health information in an IT-outsourcing context came into the national public consciousness and it has been extensively addressed by the Information and Privacy Commissioner for British Columbia and by the British Columbia Legislature. The Ontario privacy commissioner has also dealt, more recently, with IT outsourcing issues that apply directly to the establishment of a province wide EHR. These jurisdictional choices also make sense from a conceptual point of view. Ontario has health-sector-specific personal data protection legislation, the *Personal Health Information Protection Act*,[18] which has been declared substantially similar to the federal PIPEDA, and this regulates entities who are defined in the legislation as "health information custodians" ("HIC"). This designation applies to both public and private bodies and individuals. On the other hand, in British Columbia, personal information is governed, generally, in the public sector by the *Freedom of Information and Protection of Privacy Act*[19] and in the private sector by the *Personal Information Protection Act*,[20] and health information is covered by one or the other, depending on what type of organization holds it. These two jurisdictions represent two unique schemas under which personal health information is regulated in two different provinces. PIPEDA, enacted by the federal government, applies to the private sector in provinces where there is no substantially similar legislation and where information is transferred across jurisdictional borders. Consideration of PIPEDA will, therefore, provide further contrast to the other legislative schemes discussed. It is beyond the scope of

14 S.O. 2004, c. 3, Sch. A.

15 *Health Information Act*, R.S.A. 2000, Ch. H-5.

16 *Personal Health Information Act*, C.C.S.M., Ch. P33.5.

17 *Health Information Protection Act*, S.S. 1999, Ch. H-0.02.

18 *Supra* note 14.

19 R.S.B.C. 1996, ch. 165.

20 *Supra* note 12.

this article to canvas the personal data protection laws of each Canadian jurisdiction exhaustively; however, as representatives of the different legislative schemes in place in Canadian provinces, a discussion that focuses on the three jurisdictions, described above, will highlight the various elements that must be addressed when implementing an IT outsourcing agreement.

III. IT OUTSOURCING

Virtually any function performed by employees of a company can be outsourced to a third party with expertise in that particular area. Outsourcing is primarily done to cut costs. Specialized companies can often perform certain functions more cheaply than in-house employees. In the IT field, the need for specialization and training means that it is not just costs that are a consideration, but also the fact that sometimes the work cannot be done in-house to the same level of service or expertise.[21]

With respect to outsourcing of personal health information, there are a variety of schemes and formats that can be applied. For instance, the outsourcing could be done by a third party for a single organization, or the IT provider's services may be employed at a higher point in the organizational structure, for example, in connection with networks that exist between individual organizations. The function performed could be discrete and specific, such as billing a set of clients, or it could be of a more underlying structural nature, such as providing and maintaining the software and infrastructure by which an entire network operates. In addition, the manner in which data is accessed or transferred may differ. If the function of the IT provider involves data processing or storage, then data may be fully transferred to the third party and stored on its servers, completely separate from the providing organization. On the other hand, where the service provided is of a more structural nature, such as where the provider is setting up an entire system or network, then data may never even actually be transferred outside of the original organization, but may be accessed by the third party provider, for example, to enter the data into the system.[22] There could also be an in-between ground where data is transferred and stored on third party servers, but is fully accessible remotely by the providing organization. In addition to all of these permutations, it is important to bear in mind that when the information in question is personal health information, the organiza-

---

21 C. Ian Kyer, *Outsourcing Transactions: A Practical Guide* (Aurora: Canada Law Book, 2006) at 1–3.

22 The former structure described here, wherein a third party contractor receives discrete collections of data and processes it independently of the providing organization, is likely representative of an older model of information handling where companies would routinely have their data processing needs met by an external "service bureau" because personal or small scale computing was simply not available or feasible for most organizations — see Kyer, *ibid.*, at 1-2. Although this kind of one-off service provision is still prevalent, the latter structure is likely to become more widespread given the modern and increasingly greater networking capacities and the ability to construct integrated infrastructure. In the future, there is likely to be a greater demand for companies to provide data hosting services and software set-up and maintenance services.

tions involved may be either in the public sector or in the private sector or, where networking functions are the subject of the IT work being done, both.

IV. TRANSFERS OF PERSONAL HEALTH INFORMATION AND CROSS-BORDER TRANSACTIONS

(a) British Columbia

In 2004, the British Columbia provincial government began making plans to retain a contractor to run the province's public health insurance program. This plan came into the public consciousness because the organization with which the outsourcing contract was to be made was a United States based company. A lawsuit was launched by the British Columbia Public Employee's Union in the British Columbia Supreme Court protesting the proposed agreement. The main issue that emerged as a concern of the public and the media was the possibility that the personal health information of British Columbians could be accessed by the United States government by operation of the *USA Patriot Act*.[23] In response to these concerns, the Information and Privacy Commissioner for British Columbia initiated a public enquiry that received many submissions, from both national and international sources, and culminated in a report[24] that considered the operation of the *USA Patriot Act* and its implications in public sector outsourcing.

The *USA Patriot Act* was enacted by U.S. Congress in very short order after September 11, 2001. It is a piece of anti-terrorism legislation that expands the intelligence gathering and surveillance powers of American law enforcement and national security agencies.[25] The provision of the legislation that has caused the most unease in Canada, because of its potential impact even within Canadian borders, is section 215 of the *USA Patriot Act*. This section amends sections 501–503 of the U.S. *Foreign Intelligence Surveillance Act of 1978* ("FISA")[26] expanding the authority of the Federal Bureau of Investigation to make an application to a court for an order ("FISA order") requiring the production of "any tangible thing" for an investigation to protect against international terrorism. As a result of these amendments, search, seizure, and disclosure orders can be issued in circumstances that would not be sufficient to allow access by the government in Canada. The primary concern for Canadians is, of course, the possibility that a FISA order could effect disclosure of information about Canadians when an individual or organization that

---

23 *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 [*USA Patriot Act*].

24 Information and Privacy Commissioner for British Columbia, *Privacy and the US Patriot Act: Implications for British Columbia Public Sector Outsourcing* (British Columbia: Information and Privacy Commissioner for British Columbia, 2004) [B.C. Report].

25 The *USA Patriot Act* is not actually a single freestanding piece of legislation but rather is a series of amendments to other pieces of security and surveillance legislation. However, current commentary usually refers just to the Patriot Act and the amendments that it engendered.

26 50 U.S.C. 1861 *et seq.*

is subject to U.S. jurisdiction is in possession of, or has access to, that information.[27]

The Information and Privacy Commissioner's report addressed two "cross-border" scenarios that could raise *USA Patriot Act* issues. The first arises where data is actually transferred to a contracting party that is geographically within the United States. The second occurs where data remains in Canada but is in the custody of a company that is either a subsidiary of, or directly controlled by, an American company. A clear answer to the first issue warranted little discussion. Personal information is subject to the laws of the jurisdiction in which it is geographically located.[28] If those laws allow for, or require, disclosure in a given circumstance, then any contractual provisions that may provide otherwise cannot prevent disclosure.[29] On the second issue, the commission determined that, "[t]here is general consensus in the submissions that [a U.S. court] could, under FISA, order a US corporation to produce records held in Canada by its Canadian subsidiary."[30] The ability to compel such disclosure would depend on practical ability, based on the degree or extent of corporate control, to obtain and produce the information.[31] The report went on to consider the likelihood that U.S. authorities *would* use a FISA court order to access personal data held by Canadian subsidiaries of American companies. The report concluded that while other avenues such as Mutual Legal Assistance Treaties or letters of request to Canadian courts are available, they are unlikely to be used in lieu of a FISA order where such an order would be effective in accessing the information.[32] As such, the report found that there is a real possibility that U.S. authorities would use a FISA order to gain access to personal information held within Canada by a Canadian subsidiary of an American company. Nonetheless, the report concluded that "a ban on British Columbia government outsourcing of the management of sensitive personal information would not be a practical or effective plan of action."[33]

---

27 For further consideration of this topic in the outsourcing context, see Adam D. Vereshack, *A Practical Guide to Outsourcing Agreements* (Markham: LexisNexis Butterworths, 2005) at 230-231; See also BC report, *supra* note 24, at 70.

28 B.C. Report, *ibid.,* at 117.

29 Under the provisions of the *USA Patriot Act*, an organization or company that discloses information in accordance with the act, is protected from liability if such disclosure was otherwise contractually prohibited. Such limitation of liability is, of course, only applicable to a lawsuit brought within the United States and so would not protect a Canadian subsidiary from civil liability or from liability under Canadian statute.

30 B.C. Report, *supra* note 24 at 118.

31 *Ibid*, at 132. Some US courts have held that there is corporate control where a US corporation, can, directly or indirectly, elect a majority of the directors of the foreign corporation.

32 *Ibid*, at 116 and 128; But see Vereshack, *supra* note 27 at 231 where he contends that "there is a belief among certain knowledgeable Canadian and U.S. practitioners that if the United States were to require Personal Information from Canada in connection with an offence in the United States, it would be much more practical and expeditious to use the bilateral Mutual Legal Assistance Treaty, between those two countries to obtain the required information."

33 B.C. Report, *supra* note 24 at 133.

Perhaps the most significant conclusion of the report was that the provisions of the British Columbia *Freedom of Information and Protection of Privacy Act*[34] ("FOIPPA"), which regulates data protection in the British Columbia public sector were not found to be inconsistent with outsourcing generally. The outsourcing of IT functions that involve the transfer of personal information to third parties is not prohibited by FOIPPA either expressly or as a consequence of any requirement or prohibition in the Act. Every province in Canada has legislation that, like FIOPPA, regulates personal information held by provincial government organizations. Although every province has not had reason or opportunity to examine and report on how its own legislation would regulate outsourcing, where it has been considered, it has similarly been concluded that outsourcing is not prohibited outright. The same conclusion has also consistently been reached with respect to PIPEDA and other private sector legislation.[35]

However, in response to the British Columbia Public Employee's Union lawsuit and the Commissioner's report, the British Columbia legislature, in October of 2004, enacted several amendments to FOIPPA that further impact outsourcing agreements.[36] Now, under section 30.1 of FOIPPA, public sector entities are required to ensure that personal information in its custody or control is stored and accessed *only* in Canada.[37] In addition, public bodies and their third party service providers are required to refuse to disclose information in response to a foreign demand[38] and are required to report to the Minister responsible for FOIPPA any demand for information made by a foreign authority. Commentators have observed that these latter two amendments have the potential to put any U.S. linked company that might be subject to a U.S. FISA disclosure order in the position of having to disobey one jurisdiction's laws in order to comply with another's.[39] In Nova Sco-

34 *Supra* note 19

35 See Office of the Privacy Commissioner of Canada, *PIPEDA Case Summary #2005-313, Bank's notification to customers triggers PATRIOT ACT concerns* (Ottawa: Office of the Privacy Commissioner of Canada, 2005); Office of the Privacy Commissioner of Canada, *PIPEDA Case Summary #2006-333, Canadian-based company shares customer personal information with U.S. parent* (Ottawa: Office of the Privacy Commissioner of Canada, 2006); Office of the Privacy Commissioner of Canada, *PIPEDA Case Summary #2008-394, Outsourcing of canada.com e-mail services to U.S.-based firm raises questions for subscribers* (Ottawa: Office of the Privacy Commissioner of Canada, 2008).

36 *Freedom of Information and Protection of Privacy Amendment Act, 2004*, S.B.C. 2004, c. 64 [*Amendment Act*].

37 Except when cross-border access/storage is consented to by the individual in a prescribed manner (30.1(a)).

38 *Supra* note 19; This provision specifically prohibits disclosure which is not authorized by the act and subject to sections 33.1 and 33.2, which were also amended by the *Amendment Act*, *supra* note 36, such foreign orders do not constitute authorization.

39 Kyer, *supra* note 21 at 18-6; Richard Corley & Ian Hay, "Privacy and Confidentiality Issues in Outsourcing Transactions" (Powerpoint Presentation made at IT.Can & LSUC 7th Annual IT Law Spring Training Program, May 14, 2007), at slides 15-16 & 21.

tia, the *Personal Information International Disclosure Protection Act*,[40] enacted in 2006, contains similar provisions prohibiting the transfer of personal information held by the public sector outside of the country.

These provisions are significant in that they have the potential to significantly alter whether, and with whom, public sector players in these jurisdictions choose to, and are able to, contract for IT outsourcing services. However, from a regulatory and administrative standpoint, arguably, the more significant amendment to FOIPPA was to sections 30.1–30.5, which provides that the sections prohibiting disclosure, mandating notification of foreign disclosure demands and mandating that information be maintained in Canada, now apply to third party service providers as well as to the public body that originally held the information. This is significant because, previously, only public bodies were governed by the legislation and third party service providers were bound only by whatever contractual provisions were in the IT outsourcing contracts themselves.

In contrast, personal information held by private sector organizations in British Columbia is regulated by the *Personal Information Protection Act*[41] ("PIPA"). The PIPA does not contain any provision that would prohibit outsourcing of personal information, even across jurisdictional borders. In addition, unlike the amended FOIPPA, PIPA does not apply directly to third party service providers. However, PIPA does require that an organization protect information that is in its control even when the information is not within the custody of the organization, suggesting that where an organization outsources some function to a third party, it continues to be responsible for the personal information even when it is in the hands of the service provider. In this way, PIPA is more similar to the federal PIPEDA, a point that will be discussed further below.

(b) Ontario

In Ontario, the *Personal Health Information Protection Act*[42] ("PHIPA"), enacted in 2004, applies to parties who are defined as "health information custodians," which includes hospitals, doctors, pharmacists and laboratories, ambulance services and, nursing and care homes. Like the amended FOIPPA, PHIPA also contains provisions that apply directly to third party service providers. Section 2 of PHIPA defines an "agent" as an individual that, "with the authorization of the custodian, acts for, or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes." Agents are permitted to collect, use and disclose personal health information only if the health information custodian is permitted or required to do so under PHIPA.[43] It is also significant that section 6(1) of PHIPA provides that where a health information custodian provides personal health information to its own agent, this is a "use" of the information and not a "disclosure." Therefore, such a transfer must comply with

40 S.N.S. 2006, c. 3.

41 *Supra* note 12.

42 *Supra* note 14.

43 Section 17. In addition, many of the provisions of PHIPA that regulate when and how health information custodians may collect, use and disclose personal information also apply explicitly to agents of the health information custodian.

the provisions of PHIPA that regulate the uses that a health information custodian may make of personal health information[44] but is not caught by the much more strenuous rules regulating disclosure.[45] As a whole, these provisions of PHIPA treat agents of health information custodians as extensions of the custodians. Agents, themselves, are regulated by PHIPA in that many provisions of PHIPA do apply directly to them, but the specifics of what agents may do with the information they receive from custodians is regulated by the constraints of the Act that apply to the custodians, themselves.

The "agent" provisions of PHIPA could apply to many types of IT outsourcing transactions, including the kind of agreement considered by the British Columbia government, discussed above (if it were to have taken place in Ontario). Regulations made pursuant to section 10(4) of PHIPA, define a second type of service provider, a "health information network provider," as "a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another."[46] The regulations mandate the actions of the service provider and include, among other things, directives that the service provider and its employees must not use the information except as necessary in the course of providing the services, must not disclose the information, and must report to the health information custodian any unauthorized access of the information. These provisions would apply to the kind of outsourcing agreement that is implemented at the networking level, as opposed to individual one-off agreements. They would apply, for example, where the service being provided is for the implementation of an EHR.[47] A "health information network provider" could also be an "agent"[48] and therefore subject to both sets of provisions under PHIPA.

The Information and Privacy Commissioner for Ontario has had cause to consider these provisions in PHIPA in the context of an IT outsourcing agreement that raised cross-border access concerns.[49] In 2006, Cancer Care Ontario entered into an agreement with a company, Initiate Software, for the provision of software services that link personal health information to specific individuals such that access to information about that individual could be accessed across the healthcare sector. In-

44 PHIPA, *supra* note 14 at s. 37.

45 *Ibid.* at ss. 38–50.

46 Ontario Regulation 329/04, s. 6.

47 See e.g., Information and Privacy Commissioner/Ontario, *Review of the Smart Systems for Health Agency (SSHA): An Electronic Goods or Services Provider to Health Information Custodians under the Personal Health Information Protection Act, 2004* (Toronto: Information and Privacy Commissioner/Ontario, 2007). Smart Systems for Health Agency, the subject of the review was created by the Province of Ontario to provide a secure, integrated, province-wide information technology infrastructure which would be the foundation of an Ontario-wide EHR. This report considers the way in which the "health information network provider" provisions apply to this agreement.

48 Ontario Regulation 329/04, section 6(2).

49 Information and Privacy Commissioner/Ontario, *Investigation Report: PHIPA Report HI06-45 Initiate Systems Inc. and the Ontario Ministry of Health and Long-Term Care* (Toronto: Information and Privacy Commissioner/Ontario, 2006).

Q-Tel, which is the venture capital branch of the American Central Intelligence Agency ("CIA") and whose mandate it is to invest in intelligence and information gathering technology businesses, had recently invested in Initiate Software. This raised concerns in the public and the media that information to which Initiate Software was privy could be accessed by American authorities via the CIA's interest in Initiate. Unlike in British Columbia, the concern here was not with the possibility of a FISA order under the *USA Patriot Act*, but rather the potential for a more direct access by a controlling foreign body (which, in this case, happened to be a foreign governmental organization). Here, the Information and Privacy Commissioner for Ontario found that Initiate Software was an "agent" of Cancer Care Ontario, as defined by PHIPA and that the agreement between the two parties recognized this arrangement. The services provided by Initiate were limited to configuring the software, uploading the information and providing troubleshooting assistance. Initiate performed no remote data hosting or processing functions. In addition, the agreement provided Initiate Software with very limited access to personal health information of Ontarians since all work done by Initiate was performed at Cancer Care Ontario sites under the direct supervision of the information custodian, and there was no capacity for remote access to the system. The Commissioner concluded that, "personal health information [was] not being collected, used, or disclosed in contravention of PHIPA through the use of Initiate Software in Ontario, nor [did] any health information leave the province."[50] The contractual provisions contained in the IT outsourcing agreement between Initiate and Cancer Care Ontario were of great importance to the Commissioner in this case, and it was by these provisions, and practical confirmations that they were being complied with, that the Commissioner determined that the agreement was in compliance with PHIPA.

(c) PIPEDA

As discussed above, personal health information is governed differently in different jurisdictions. The discussion above has focused on British Columbia and Ontario as representative of two different schemes. In Ontario, PHIPA applies to both public and private sector organizations who are defined as health information custodians. In British Columbia, FOIPPA regulates public sector organizations while PIPA applies to private sector organizations. However, the majority of provinces do not have provincial private sector personal data protection legislation. In these provinces, the federal PIPEDA applies to such organizations. PIPEDA also applies as soon as information crosses a border. Therefore, a consideration of an IT outsourcing agreement that deals with information that is subject to PIPEDA must be considered.

In January of 2009, the Office of the Privacy Commissioner of Canada ("Commissioner") published *Processing Personal Data Across Borders Guidelines* to "explain how the PIPEDA applies to transfers of personal information to a third

50 *Ibid.* at 10. There is no indication as to whether the Commissioner would have decided differently if the information had left the province. PHIPA, unlike FOIPPA, does not specifically prohibit this and the finding that the information did not leave the province was central to reasons issued by the Commissioner in this case.

party, including a third party operating outside of Canada, for processing."[51] These guidelines summarize several years of decisions by the Commissioner on this point.[52] The guidelines highlight Principle 4.1.3 of Schedule 1 of PIPEDA, which provides that, "[a]n organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party." Principle 4.1.3 specifically authorizes third party service provider agreements but mandates that: (1) the original organization remains responsible for the information, and (2) if it enters into agreements with third parties, then the contractual provisions must ensure that the third party provides the same protections required of the original organization by PIPEDA.

PIPEDA, unlike FOIPPA or PHIPA, does not directly apply to the third parties. As is the case with PIPA, the third party providers are subject only to contractual restrictions and not legislative ones. The guidelines confirm that, as under PHIPA, disclosure to a third party is a "use" of the information and not a "disclosure," although it is not explicitly stated as such in PIPEDA.

The guidelines recognize that when information is transferred to foreign jurisdictions, it is subject to the laws of these jurisdictions, and where disclosure is required under the law of the foreign jurisdiction, this can always override contractual provisions that purport to prevent disclosure to foreign authorities. Nonetheless, PIPEDA does not prohibit or restrict such a cross-border transaction. The guidelines intimate — but do not explicitly state — that in some instances the risk of disclosure in a foreign jurisdiction might be too great and, especially where the information is highly sensitive, a private sector organization governed by PIPEDA ought not to enter into a cross-border information transfer agreement. Transfers of health information, which is among the most sensitive and private of personal information, could well be just the sort of information that the guidelines contemplate on this point, although this is not explicitly stated.[53] However, it seems clear that it is up to the discretion of the individual organization as to whether the personal information that they hold is too sensitive, or the risk of disclosure too high to enter into a cross-border agreement. PIPEDA does not prohibit it.

On the whole, private sector organizations whose personal information is governed by PIPEDA (or substantially similar provincial legislation such as the British Columbia PIPA), are subject to many of the same provisions and restrictions regarding use and disclosure in the context of third party IT outsourcing agreements

---

51 PIPEDA Guidelines, *supra* note 1 at 2.

52 See *supra* note 35; Office of the Privacy Commissioner of Canada, *SWIFT investigation report addressing disclosure of Canadian banking information to the U.S. Treasury* (Ottawa: Office of the Privacy Commissioner of Canada, April 2, 2007); Office of the Privacy Commissioner of Canada, *Transferring Personal Information about Canadians Across Borders — Implications of the USA PATRIOT Act* (Ottawa: Office of the Privacy Commissioner of Canada, 2004).

53 The guidelines *do* consider financial information that is also highly sensitive and akin, in some ways, to health information.

as are public sector organizations under provincial legislation such as FOIPPA, or health sector specific legislation like PHIPA. All organizations are free to enter into contracts with third parties for information technology outsourcing or other services. In all cases, transfer of information to these third parties is a "use" of the information and not a "disclosure," recognizing that the outsourced functions are still part of the overall operation of the original organization. The parties to whom the information is transferred are limited in what they can do with it. They can use the information only for the purposes for which the original organization has been authorized and for the purposes for which they are retained contractually by the original organization. However, under PIPEDA or substantially similar legislation, these restrictions on third parties must be enforced primarily by contractual provisions alone, while under FOIPPA or PHIPA, the third party service providers are, themselves, regulated (although contractual provisions are still very important to establish compliance with the legislation). In addition, provincial public sector legislation such as FOIPPA in British Columbia, and Nova Scotia's *Personal Information International Disclosure Protection Act*,[54] specifically prohibit the transfer or storage of personal information outside of Canada. On the other hand, neither PIPEDA nor any substantially similar legislation prohibit such transactions.

CONCLUSION

When a Canadian organization that has personal health information is contemplating entering into an IT outsourcing agreement that would involve that personal health information being either transferred to, or accessed by a third party IT service provider, there are a number of issues that must be considered. The specific pieces of legislation and the case studies discussed in this paper have highlighted some of the most significant of these issues.

It is clear that IT outsourcing is not prohibited outright by any personal data protection legislation. However, in some jurisdictions, specifically the public sector in British Columbia and Nova Scotia, there are restrictions on the kind of outsourcing agreement that can be entered into, since data cannot be stored or accessed outside of Canada. In such a case, restrictions are imposed on the possible structure of the putative agreements. Even where data is stored only in Canada, parties to outsourcing agreements that deal with public sector information in these provinces may face compliance conflicts between laws of different jurisdiction where the third party service provider is corporately linked to a foreign company. Such a party would have to consider whether the risk of such a conflict is worth the potential benefits of the contract.

There are other circumstances where it may not be advisable to enter into a cross-border transaction, even though it may be allowed. If the information is particularly sensitive, then the potential harm that could result from a forced foreign disclosure may outweigh the benefits of the cross-border agreement. If such a transaction is not prohibited, the harms to be considered are more diverse than simple legal repercussions and may include loss of business reputation, client dissatisfaction, and public outcry if disclosure were to occur. Again, a cost/benefit analysis must be performed by the parties.

54 *Supra* note 40.

It is clear that in any outsourcing agreement wherein personal information is transferred, appropriate contractual provisions are of paramount importance. If the information falls within the purview of PIPEDA, contractual provisions are the primary mechanism for controlling the actions of the third party. Appropriate contractual provisions allow an organization to meet its own obligations under the legislation to protect the information, even when it is in the hands of a third party. Where the third party service provider is itself regulated by the applicable personal data protection legislation, comprehensive contractual provisions are still necessary to demonstrate compliance with the legislation and to establish the nature of the relationship between the parties.

Contractual provisions should be specific. A third party service provider will be hesitant or unwilling to accept vague provisions that merely require, for example, "compliance with all applicable laws,"[55] since it is the original organization that is most familiar with the law and its operation in the specific context. Specificity of contractual provisions is especially important under PIPEDA when the onus is on the original organization to ensure that a "comparable level of protection" is afforded the information. It is important to be specific as to what that level is, and how it is achieved.

All of these considerations are essential when an organization is deciding on the appropriate structure and contractual obligations in an IT outsourcing agreement. However, even when all of these issues are appropriately and comprehensively addressed, they mitigate, but do not fully eliminate the risk of disclosure of personal health information subject to the operation of a foreign law that binds a third party IT service provider. Nonetheless, Canadian personal data protection legislation and the judicial and administrative interpretation of it thus far, recognize that outsourcing agreements are a necessity and an inevitability in the technological evolution of data management, and especially infrastructure, development. Careful and appropriate management of these outsourcing and data management and transfer agreements must be in place to realize the potentially life saving and health-care enhancing benefits of EHRs, while maintaining the security and privacy of the most sensitive of personal information.

55 Kyer, *supra* note 21.