Health Law

Coming Soon to a Health Sector Near You: An Advance Look at the New Ontario Personal Health Information Protection Act (PHIPA): Part II

John P. Beardwood and J. Alexis Kerr

This is Part II of a two-part article that provides a broad overview and comparative study of the new Ontario health sector-specific privacy legislation. In Part I, which appeared in the previous issue of *Healthcare Quarterly*, we discussed the objectives, structure and scope of, as well as the substantive rights and obligations created by, the new Ontario Act. In Part II, we discuss the administrative obligations created by the Ontario Act, as well as the provisions relating to the enforcement of, and remedies available under, the Act. We also contrast the Ontario Act with the various approaches to the protection of personal health information that has already been adopted by other provinces, including Alberta, Saskatchewan and Manitoba.

Introduction to Part II

As of the publication date of Part I of this article, the *Personal Health and Information Privacy Act* (PHIPA)[1] – which, together with the *Quality of Care Information Protection Act*,[2] forms the *Health and Information Privacy Act* (HIPA)[3] – had received Royal Assent, but had yet to enter into force. This changed on November 1, 2004, when both PHIPA and its associated general regulation ("Regulation")[4] officially took effect. In addition to creating those substantive rights and obligations in respect of the protection of personal health information that we canvassed in Part I, PHIPA and the Regulation together impose certain administrative obligations on health information custodians (HICs), and establish a regime of enforcement and related remedies.

A. Administrative Obligations

PHIPA imposes a number of logistical and administrative obligations on HICs.

1. Information Practices Generally

PHIPA articulates the high-level principle that each HIC that has custody and control of personal health information must establish and implement information practices that comply with PHIPA.[5]

2. Contact Person and Public Statement

An HIC must designate a contact person who is authorized to facilitate the HICs' compliance with PHIPA, ensure that all

1. S.O. 2004, c. 3 Sched. A.
2. S.O. 2004, c. 3 Sched. B.
3. S.O. 2004, c. 3.
4. Personal Health Information Protection Act, 2004, General Regulation, O. Reg. 329/04, which we referred to in Part I of this article as the Proposed Regulation.
5. S.10, PHIPA.

agents of the custodian are appropriately informed of their duties under PHIPA,[6] respond to inquiries from the public about the custodian's information practices, respond to access/correction requests and receive complaints from the public regarding contraventions of PHIPA. In addition, each HIC must make available to the public a written statement that provides a general description of the custodian's information practices, describes how to reach their contact person and how an individual may access, correct or make a complaint regarding their personal health information.[7]

3. Accuracy

Each HIC must take reasonable steps to ensure that the information it uses about an individual is as accurate, complete and up-to-date as is necessary for the purposes, and where disclosing such information, shall clearly set out for the recipient of the information the limitations on the accuracy, completeness or up-to-date character of the information.[8]

4. Security

PHIPA requires each HIC to take reasonable steps to ensure that personal health information in the custodian's control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or destruction.[9] There are also specific provisions regarding the appropriate handling and storage of personal health information records.[10] It is worthy of note, however, that subject to one exception,[11] there are no specific time periods for retention of such records; rather, "A Guide to the *Health Information Protection Act*" issued by the Information and Privacy Commissioner of Ontario in September 2004 advises each HIC to refer to other existing legislation that sets out such requirements.

5. Notice Requirements

In a significant divergence from PIPEDA, generally each HIC that has custody or control of personal health information must *notify* the individual affected at the first reasonable opportunity if personal heath information under its control is (a) stolen, lost or accessed by unauthorized persons,[12] or (b) subject to certain exceptions, used or disclosed without the individual's consent, in a manner that is outside the scope of the HIC's description of its information practices set out in its public statement.[13] Note that in the latter case the current language does not appear to require such notification where the information is used or disclosed without consent, but such use and disclosure is congruent with the HIC's privacy statement. In effect, PHIPA treats the public statement as a quasi-representation to the public as to how it will use the information, which, if breached, requires that the HIC notify the affected individuals of such breach.

6. Access

PHIPA gives an individual the general right to access any record containing his or her personal health information that is controlled by an HIC except under certain enumerated circumstances.[14] Subject to (a) certain permissible extensions, and (b) the right of an individual to apply to the Information and Privacy Commissioner of Ontario for a reduction in this time period, the request must be processed no later than 30 days after its receipt. If the custodian refuses or is deemed to refuse access, the individual may file a complaint with the Privacy Commissioner. Unless the regulations stipulate a higher amount, when disclosing personal health information, an HIC is limited to charging fees equal to the amount of reasonable cost recovery.[15]

---

6. S.15, PHIPA.
7. S.16, PHIPA.
8. S.11, PHIPA.
9. S.12(1), PHIPA.
10. SS.13 and 14, PHIPA.
11. S.13(2), PHIPA: a health information custodian that has custody or control of personal health information that is the subject of a request for access shall retain the information for as long as necessary to allow the individual to exhaust any recourse under this Act that he or she may have with respect to the request.
12. S.12(2), PHIPA.
13. The HIC must also make a note of the uses and disclosures, and keep the note as part of the records of personal health information about the individual that it has in its custody.
14. For example, the individual has no right of access where "granting the access could reasonably be expected to result in a risk of serious harm to the treatment or recovery of the individual or a risk of serious bodily harm to the individual or to another person": s.50(1)(e)(i). In addition, the Regulation exempts from the access and correction provisions of PHIPA (a) personal health information that a researcher holds solely for the purpose of research that is conducted in accordance with PHIPA; (b) under certain circumstances, personal health information in the custody or control of a laboratory; and (c) personal health information contained in a record that is dedicated primarily to the personal health information of another person: s. 24.
15. S.52, PHIPA.

B. Enforcement and Remedies

1. How Is the PHIPA to Be Enforced?

The Commissioner under PHIPA is the Information and Privacy Commissioner appointed under the *Freedom of Information and Protection of Privacy Act* (Ontario), the existing legislation governing freedom of information and the privacy of personal information collected, used or disclosed in the Ontario public sector.

2. Making and Reviewing Complaints

A person who has reasonable grounds to believe that another person has contravened or is about to contravene a provision of PHIPA may make a complaint to the Commissioner,[16] and/or the Commissioner may initiate a review on his or her own initiative,[17] where there are reasonable grounds to believe that another person has contravened or is about to contravene a provision of PHIPA, and that the subject matter of the review relates to such contravention. In the case of a person-initiated complaint, the Commissioner may in his or her discretion decide not to review the subject matter of the complaint. After conducting such a review, and in contrast to the powers of the federal privacy commissioner under PIPEDA, the Commissioner has certain enumerated order-making powers.[18] These include the power to order the HIC to provide access to or correct the personal health information in question, and to modify, cease, not commence or implement an information practice. It is worthy of note that the Commissioner may make a copy of this order available to, in addition to the complainant and the subject of the complaint, "any other person whom the Commissioner considers appropriate." It remains a question whether the Commissioner could publicly disclose the order under this provision.

3. Offences

The list of enumerated offences under PHIPA is lengthy and includes where a person: wilfully collects, uses or discloses personal health information in contravention of PHIPA; makes a request under PHIP under false pretences for access to or correction of a record of personal health information; disposes of a personal health information record in the custody or under the control of the HIC after receiving a request for access to the record, with intent to evade such request; misuses health card numbers; wilfully obstructs the Commissioner or an authorized agent of the Commissioner in the performance of his or her functions; or dismisses, suspends, demotes, disciplines, harasses or otherwise disadvantages a person who has refused to contravene PHIPA or who has alerted the Commissioner to a contravention of PHIPA.

4. Penalties

Damages

A person affected by an order may appeal on a question of law to the Divisional Court. Where (a) an order has made been made final – that is, as the result of there being no further right of appeal, or (b) a person is finally convicted of an offence – again, final as a result of there being no further right of appeal – a person may commence a proceeding in the Ontario Superior Court of Justice for damages for actual harm that the person has suffered as a result of the breach of PHIPA. If the Court determines that the breach or offence was engaged in by the defendants wilfully or recklessly, the Court may include in its award of damages an award of up to $10,000 for mental anguish.[19]

Fines

PHIPA provides for significant fines for both individuals and organizations, with individuals liable for fines up to $50,000 and corporations liable for fines up to $250,000.

Personal Liability

If a corporation commits an offence under PHIPA, every officer, member, employee or other agent of the corporation who authorized the offence or had the authority to prevent the offence from being committed but knowingly refrained from doing so, is deemed a party to the offence and is *personally liable*, on conviction, to the penalty for the offence. It is important to note that this applies *whether or not the corporation has been prosecuted or convicted.*

C. Other Approaches to Protecting Personal Health Information

The following comparative review outlines at a high level some of the common principles PHIPA shares with the legislation of other jurisdictions applicable to personal health information, as well as some of the variances between such legislation and PHIPA. Through necessity, the list of common and differing principles in each case is intended to be illustrative rather than exhaustive.

1. Manitoba, Saskatchewan and Alberta

In addition to Ontario, Manitoba, Saskatchewan and Alberta are the only provinces that have enacted health sector-specific privacy legislation.

17. S.54, PHIPA.
18. S.56, PHIPA.
19. S.60, PHIPA.

The Manitoba *Personal Health Information Act* (Manitoba Act),[20] which was the first statute in Canada to deal with the privacy of personal health information in both the public and private sectors, came into force in December 1997. The *Saskatchewan Health Information Protection Act* (Saskatchewan Act),[21] which received Royal Assent on May 6, 1999, was finally proclaimed in force, with some exceptions, in September 2003. The *Alberta Health Information Act* (Alberta Act) came into force in April 2001.[22] In addition to the Alberta Act, the application of which is generally limited to organizations that receive funding from the Alberta Health Care Insurance Plan, Alberta has also enacted general private sector privacy legislation, entitled the *Personal Information Protection Act* (PIPA Alberta).[23] PIPA Alberta fills the gap left by the Alberta Act by regulating the collection, use and disclosure of health information for non-healthcare related purposes (e.g., the employment context) and by private-sector organizations that are not subject to the Alberta Act.[24]

Common Principles: Trustees/Custodians and the Circle of Care

Like the Ontario PHIPA, each of the Manitoba, Saskatchewan and Alberta Acts distinguish between entities that operate within the "circle of care" and all other entities that may collect, use and disclose personal health information. Under the Manitoba and Saskatchewan Acts, the "circle of care" entities are referred to as "trustees," while under the Alberta Act, such entities are referred to as "custodians." Notwithstanding the differences in terminology, however, these Acts share a common objective: to protect the privacy of an individual's personal health information ("health information" under the Alberta Act), while at the same time facilitating the effective operation of the healthcare system.

In light of this objective, the Acts are similar to the Ontario PHIPA, in that they (a) create a general right of access to, and correction of, an individual's personal health information by the individual; (b) establish specific requirements in relation to the collection, use and disclosure of personal health information by the "circle of care" entities, which include rules relating to the disclosure of such information to non-"circle of care entities"; and (c) impose specific obligations with respect to the retention, security and destruction of personal health information that is in a "circle of care" entity's custody or under its control.

In addition, each of these Acts contains specific provisions relating to the collection, use and disclosure of personal health information in the research context.

Common Principles: Lockbox Principle in the Saskatchewan Act

The Saskatchewan Act is the only other statute specific to the health sector that contains a provision similar to the "lockbox" principle in the Ontario PHIPA. Section 7 of the Saskatchewan Act permits an individual to revoke his or her consent to a trustee or its agent's collection, use or disclosure of personal information, and a trustee is required to take all reasonable steps to promptly comply with the revocation. The revocation does not, however, have any retroactive effect.

Variances: No Specific Mechanisms in the Acts re Fundraising or Marketing

Unlike the Ontario PHIPA, these Acts do not specifically address the collection, use and disclosure of personal health information in the context of fundraising or marketing, which means that such information may only be collected, used or disclosed for such purposes with the individual's informed consent. In this respect, it is worth noting that the Alberta Act creates an offence in respect of the use of "individually identifying health information to market any service for a commercial purpose or to solicit money unless the individual who is the subject of the health information has specifically consented to its use for that purpose." [25]

Variances: More Detailed Mechanisms in the Acts re Disclosures of Personal Health Information

The Manitoba Act, which applies only to personal health information in recorded form, includes specific provisions relating to the provision of personal health information to an "information manager,"[26] and to the sale of personal health information.[27] It also requires all trustees to have written policies

20. S.63, PHIPA.

21. S.M. 1997, c. 51 (C.C.S.M., c. P33.5).

22. S.S. 1999, c. H-0.021, proclaimed in force September 1, 2003 (except subsections 17(1), 18(2) and (4) and section 69) as amended by S.S. 2002, c. R-8.2; and S.S. 2003, C. 25.

23. R.S.A. 2000, c. H-5.

24. S.A. 2003, c. P-6.5.

25. In virtually all respects that are relevant to the protection of health information in particular, the provisions of PIPA Alberta are either similar or identical to the provisions of British Columbia's Personal Information Protection Act, S.B.C. 2003, c. 63, which we discuss in the following subsection of this article.

26. S.107(2)(f), Alberta Act.

27. S.27, Manitoba Act.

and procedures relating to (a) the security,[28] and (b) the destruction[29] of personal health information. Each employee and agent of a trustee is required to sign a pledge of confidentiality acknowledging that he/she/it is bound by the security policies and procedures, and is aware of the consequences of breaching them.[30] In this respect, it is noteworthy that one of the results of the recent all-party review of the Alberta Act mandated by s. 109 of the Act[31] was the recommendation of the Select Special Health Information Act Review Committee that Alberta Health and Wellness, the ministry responsible for the Act, also consider the need for information manager provisions, information manager agreements, the application of such provisions to custodians who are also information managers and the relationship between information manager provisions and affiliate provisions.

The Saskatchewan Act applies to personal health information in any form, including both paper records and electronic records that are contained in the Saskatchewan Health Information Network. Like the Manitoba Act, the Saskatchewan Act includes specific provisions relating to the provision of personal health information to an "information management service provider."[32] Unlike the Manitoba Act, however, the Saskatchewan Act does not address the issue of the sale of personal health information, although it does permit the disclosure of such information without consent to a "successor" trustee.[33]

Variances: Distinction between Identifying and Non-Identifying Information in Alberta Act

The Alberta Act is the only privacy legislation specific to the health sector that distinguishes between, and creates rules in respect of, "individually identifying" health information and "non-identifying" health information.[34] As a corollary, the Alberta Act is also unique in its regulation of the practice or data-matching.[35] In general, the ability of a custodian to collect, use and disclose individually identifying health information is more restricted than the ability to collect, use and disclose non-identifying health information. Where, however, a custodian seeks to disclose non-identifying health information to a non-custodian, the Alberta Act requires the custodian to inform the non-custodian that it is required to inform the Alberta Information and Privacy Commissioner of its intention to use the information for the purpose of data-matching prior to using the information for that purpose.[36]

Variances: Distinction between Recorded and Non-Recorded Information in Alberta Act

Further, the Alberta Act treats unrecorded health information in a different manner than recorded health information, in that it limits a custodian's ability to use and disclose certain types of unrecorded health information only to the purpose for which the information was originally provided to the custodian.[37]

2. British Columbia

British Columbia has chosen not to enact privacy legislation specific to the health sector. It has instead opted to regulate in this area by way of its general public sector privacy legislation, the *Freedom of Information and Protection of Privacy Act* (FOIPPA),[38] and its general private sector privacy legislation, the *Personal Information Protection Act* (PIPA B.C.).[39]

FOIPPA

The focus of FOIPPA, which came into force in 1993, is two-pronged: Part 2 of the Act addresses the concept of freedom of information, while Part 3 of the Act addresses the protection of personal information. Note, however, that the individual's right to access his or her personal information is addressed in Part 2 of the Act, which also creates a broader right to access records that are in the custody or under the control of public bodies. [40]

28. Personal Health Information Regulation, Man. Reg. 245/97, registered December 11, 1997, s, 2. ("Manitoba Regulation").
29. S.17, Manitoba Act.
30. S.7, Manitoba Regulation.
31. The Final Report of the Select Special Health Information Act Review Committee was released in October 2004, and is available online: http://www.assembly.ab.ca/HIAReview/hiawebreport.pdf: see Recommendation #42.
32. S.18, Saskatchewan Act.
33. S.27(4)(c), Saskatchewan Act.
34. S.1(1)(p) & (r), Alberta Act.
35. See S.1(1)(g) and SS.68-72, Alberta Act.
36. S.32(2), Alberta Act.
37. See. SS.29 & 44, Alberta Act.
38. R.S.B.C. 1996, c. 165.
39. S.B.C. 2003, c. 63.
40. S.4(1), FOIPPA.

Variances: More Limited Application

FOIPPA purports to protect "personal information" contained in records that are in the custody or under the control of a "public body." This protection extends to a public body's collection, use and disclosure of such information. FOIPPA defines personal information as "recorded information about an identifiable individual," which implies that it does not apply to the oral exchange of information.[41] It is clear, however, that this definition encompasses personal health information in recorded form.

Similarly, the broad definition of "public body" expressly includes the Ministry of Health, hospitals, mental health facilities and various health authorities, boards and commissions. [42] It also includes the governing bodies of several designated self-regulating professions, such as the College of Physicians and Surgeons, the College of Dental Surgeons and the College of Pharmacists. Further, while FOIPPA does not generally regulate the information practices of private sector entities, such as private laboratories and the private practices of individual health practitioners, it does apply to such entities in circumstances where information that is in the physical custody of the private entity is deemed to be under the control of the public body. In this respect, public bodies[44] are precluded from circumventing the protections created by FOIPPA by merely contracting out certain of their functions to a private sector entity.[45]

Common Principles: Limits Collection, Use and Disclosure

FOIPPA reflects the fair information practices that underlie most other Canadian privacy legislation. Specifically, FOIPPA limits the ability of public bodies to collect, use and disclose personal information, in part by stipulating that personal information must either be collected directly from the individual or from another source only with the authorization of that individual, the Information and Privacy Commissioner of British Columbia or another enactment. With respect to the collection of personal health information, however, it is worth noting that FOIPPA specifically permits the collection of personal information from a source other than the individual without authorization where the collection is necessary for the medical treatment of an individual and (a) it is not possible either to collect the information directly from that individual or from another source with the authorization that is otherwise normally required.[46] Similarly, a public body may disclose personal information without authorization where the disclosure is required to contact the next of kin or friend of an injured, ill or deceased individual; or where the head of a public body determines that compelling circumstances exist that affect anyone's health or safety.[47]

Common Principles: Specific Provisions re Research

FOIPPA also contains specific provisions that regulate the collection, use and disclosure of personal information by a public body for research purposes, including medical research, clinical trials and so on.

Common Principles: Administrative Obligations

In addition to its substantive requirements, FOIPPA also imposes a number of administrative obligations on public bodies, which relate to the accuracy, retention, security, correction of and provision of access to personal information. Notably, a public body is required to retain personal information for at least one year after it has been used to make a decision about the individual.[48]

PIPA B.C.

Variances: Exclusion of Legislative Overlap

Until January 1, 2004, when PIPA B.C. came into force, the information practices of private sector entities were generally unregulated by statute, except as otherwise noted above (see A. FOIPPA, above). PIPA B.C. addresses the potential intersection between itself and FOIPPA, which results from the application

41. Schedule 1, FOIPPA.
42. Schedule 1, FOIPPA.
43. Schedule 3, FOIPPA.
44. S. 3, FOIPPA.
45. Most recently, the regulation by FOIPPA of the ability of public bodies to outsource personal information-related functions to private sector organizations has been subject to amendment as a result of concerns raised by the B.C. Government Employees Union over the possible disclosure, without knowledge or consent, of private citizens' personal information – including health information – to US authorities pursuant to certain provisions of the US Patriot Act. This concern of BCGEU stemmed from a provincial government proposal to outsource certain database services relating to the province's public health insurance scheme to a US-linked service provider, and has resulted in the amendment of FOIPPA in several respects, including the stipulation that personal information must be stored and accessed only in Canada, subject to specific exceptions set out in the Act.
46. S.27(1)(a.1), FOIPPA.
47. S.33(p) & (q), FOIPPA.
48. S.31, FOIPPA.

of FOIPPA to certain information in the physical custody of private sector entities, by clarifying that it does not apply to any personal information to which FOIPPA applies.[49] This is in notable contrast to the interaction between PHIPA and the *Personal Information Protection and Electronic Documents Act* (PIPEDA) in Ontario; in that case, Industry Canada has confirmed in its on-line guide "PIPEDA Awareness Raising Tools" (defined as PARTS) that some entities, such as private practitioners and commercial laboratories, will be caught by both PIPEDA and PHIPA.

Common Principles: Broad Definition of Personal Information to Include Oral Information

PIPA B.C. defines personal information more expansively than FOIPPA by removing the condition that the information be in recorded form. Under PIPA B.C., personal information means "any information about an identifiable individual," but does not include business contact information or work product information. Again, this definition is clearly broad enough to encompass personal health information.[50]

Common Principles: Limits Collection, Use and Disclosure

In most respects, the obligations imposed by PIPA B.C. are similar to those imposed by FOIPPA, as it relates to the collection, use, disclosure, retention, security and correction of and access to personal information. In general, PIPA B.C. limits a private sector entity's collection, use and disclosure of personal information to the amount and type of information that is necessary to fulfill a reasonable purpose. It requires that such collection, use and disclosure take place only with the knowledge and consent of the individual whom the information is about, subject to certain enumerated exceptions. One such noteworthy exception is that personal information may be collected, used or disclosed with knowledge and consent where necessary for the medical treatment of an individual who is unable to consent (collection) or who lacks the legal capacity to consent (use and disclosure).[51]

PIPA B.C. also requires each private sector entity to provide an individual with access to his or her personal information upon request, subject to enumerated mandatory and discretionary exceptions. One such exception prohibits private sector entities from disclosing personal information to an individual where such disclosure could reasonably be expected to cause or threaten immediate or grave harm to the safety or physical or mental health of either the individual who made the request, or of another individual.[52]

Common Principles: Specific Provisions re Research

In addition, PIPA B.C. contains specific provisions relating to the disclosure of personal information without consent for research purposes.[53]

3. Quebec

Quebec has not enacted privacy legislation specific to the health sector. However, the protection of personal health information is encompassed by a number of different statutes. Quebec has enacted both specific public sector personal health information and more omnibus general personal information legislation.

An Act Respecting Health Services and Social Services

More specifically, personal health records held by either public or private health and social services institutions are primarily governed by *An Act respecting Health Services and Social Services,*[54] and its attendant regulations, which regulate access to the records of the users of the various health services and social services in Quebec. This *Act* applies to public and private health institutions, but does not apply to the private practices of individual healthcare practitioners, including where such practitioners operate their practices in partnership with one another. Similarly, the Act does not apply to the collection, use or disclosure of personal health information by other types of private enterprises, which seemingly leaves a rather large gap in terms of the protection of personal health information in Quebec.

An Act Respecting the Protection of Personal Information in the Private Sector

This gap in protection is filled by the Quebec general private sector privacy legislation, *An Act Respecting the Protection of Personal Information in the Private Sector* (Private Sector Act).[55] This Act, which has been in force since 1994, does not specifically define personal health information. However, it does define personal information broadly enough – namely, "any information which relates to a natural person and allows that person to be identified"[56] – to encompass such information. Further, the *Act* applies to the collection, use, disclosure and retention of personal information by a person "in the course of carrying on an enterprise" in Quebec.[57] An "enterprise" includes most private sector entities, as well as a number of not-for-profit entities.

Note, however, that the Act does not apply to professional colleges, such as the College of Physicians and Surgeons,[58] nor does it apply to personal information held by public bodies or information held by an enterprise for or on behalf of a public body. [59]

49. S.3(2)(d), PIPA B.C.
50. S.1, PIPA B.C.
51. See SS.12(1)(b), 15(1)(b) and 18(1)(b), FOIPPA.
52. S.23(4)(a) & (b), PIPA B.C.
53. S.21(1), PIPA B.C.
54. R.S.Q., c. S-4.2.
55. R.S.Q., c. P-39.1.
56. S. 2, Private Sector Act
57. S.1, Private Sector Act.
58. See Dupré v. Comeau, [1997] R.J.Q. 439 (S.C.).
59. S.3, Private Sector Act.

In addition to adhering to what are commonly considered "fair information practices," several provisions of the Private Sector Act have specific relevance to the protection of personal health information.

For example, although personal information may generally be collected either directly from, or with the consent of, the individual whom the information is about, a person carrying on an enterprise may collect the individual's personal information from a third party without consent if "the information is collected in the interest of the person concerned and cannot be collected from him in due time." [60]

Similarly, a person carrying on an enterprise may disclose personal information without consent "to a person to whom the information must be communicated by reason of the urgency of a situation that threatens the life, health or safety of the person concerned,"[61] or "to a person who is authorized to use the information for study, research or statistical purposes."[62] Section 21 of the Act sets out the pre-conditions for being granted the required authorization.

Finally, with respect to access to personal information, the Private Sector Act contains several provisions that relate specifically to the disclosure of personal health information. This includes the obligation to communicate to an individual's family information about the cause of death or about the existence of a genetic or family disease, which is contained in the individual's medical file.[63] It also includes the ability of a person carrying on a professional healthcare enterprise to temporarily refuse an individual's access request if, in the opinion of a healthcare professional, such access could result in serious harm to the individual's health.[64]

Common Principles: Specific Provisions re Fundraising

The Private Sector Act also establishes specific rules with respect to the use of nominative lists – lists of names, addresses and telephone numbers of individuals – for the purposes of commercial or philanthropic prospection, including marketing and fundraising.[65]

4. The Rest of Canada

In the remaining provinces and territories, personal health information is protected by the applicable general provincial/territorial public sector privacy legislation, which are all, for the most part, similar to the British Columbia FOIPPA, and/or by PIPEDA for organizations (a) collecting, using and/or disclosing personal health information in the course of a commercial activity or (b) in the Northwest Territories and Nunavut.[66] As noted at the outset of the discussion of the Ontario PHIPA, with respect to the collection, use and disclosure by private sector organizations of personal information contained in medical records, the information contained in such records is almost always considered to be sensitive personal information for the purposes of PIPEDA. Accordingly, a private sector organization operating in a province/territory where PIPEDA applies will generally be required to obtain express consent prior to collecting, using or disclosing such information.

Conclusion

This comparative overview of PHIPA against the personal health information legislation in other Canadian jurisdictions serves to highlight that, while there are certain key principles that are common between PHIPA and such other legislation (for example, the fair information principles, and the intention that the provision of care not be hindered by the protection of privacy), there are also some significant differences (for example, with respect to the treatment of fundraising). For the majority of public sector custodians whose operations are limited to only one jurisdiction, the variances between jurisdictions will generally be of academic interest only. Unfortunately, private sector providers in the health sector that have national operations are not so fortunate, and need to be aware both of the jurisdictions in which such providers have obligations, and the nature of those obligations.

---

60. S.6(1), Private Sector Act.
61. S.18(7), Private Sector Act.
62. S.18(8), Private Sector Act.
63. S.31, Private Sector Act.
64. S.37, Private Sector Act.
65. SS.22-26, Private Sector Act.
66. See S.N.S. 1993, c. 5; S.P.E.I. 2001, c. F-15.01; S.N.B. 1998, c. P-19.1; R.S.Y. 2002, c. 1; and S.N.W.T. 1994, c. 20, which applies to both the Northwest Territories and Nunavut. Note that the "commercial activity" threshold established by PIPEDA effectively means that the personal health information practices of private sector, not-for-profit entities operating in Newfoundland, Nova Scotia, P.E.I., New Brunswick, Nunavut, Northwest Territories and the Yukon remain unregulated by any form of privacy legislation in relation to their non-commercial activities, for example, with respect to fundraising.