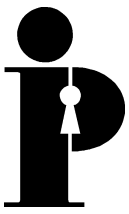
Information
and Privacy
Commissioner/
Ontario

Submission to the Ministry of Consumer and Business Services:

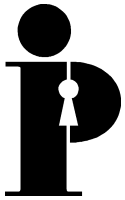
Consultation Draft

of the

Privacy of Personal Information Act, 2002



Ann Cavoukian, Ph.D.
Commissioner
February 27, 2002



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

This publication is also available on the IPC website.

Table of Contents

Introduction

The Information and Privacy Commissioner of Ontario (IPC) has a mandate under the *Freedom of Information and Protection of Privacy Act* (FIPPA) to review and comment on the privacy implications of proposed legislation.

The *Privacy of Personal Information Act, 2002* will have a significant and beneficial impact on the privacy of every individual in the province of Ontario. It will also necessitate a change in business practices at those organizations, in the broader private and health sectors, not already appropriately addressing the privacy concerns of their employees, patients and customers.

The IPC supports the government's efforts to develop and implement Ontario-specific privacy legislation. We have always believed Ontario should have its own legislative scheme, and are particularly pleased with the broad scope of the proposed legislation. We also fully support the goal of aligning Ontario's privacy regime with the federal legislation governing the private sector. Harmonization is essential to making privacy legislation across Canada easier to understand and implement.

The need for Ontario's legislation to be substantively similar to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) was brought into sharper focus with the recent determination by the European Communities of the adequacy of that Act in terms of Article 25 of the *European Directive 95/46/EC*.

After the disappointment of the proposed *Personal Health Information Privacy Act, 2000* (Bill 159), the IPC supports the Ontario government's efforts to create a single comprehensive piece of legislation covering both the private and health sectors. The need for an effective framework to protect personal health information has been acknowledged since 1980, with the publication of the *Report of the Royal Commission on Confidentiality of Health Information in Ontario* (the Krever Commission Report).

We are very pleased to see protection of privacy remains a top priority for this government. The IPC commends the government for consulting with key stakeholders and the public on this critical piece of legislation.

This submission contains our comments on ways to improve the draft legislation. They generally follow the order of questions in the consultation draft distributed by the Ministry of Consumer and Business Services (MCBS). The relevant section and page numbers from the consultation draft are included here for ease of reference.

General Questions (page iv)

1. Simplifying the Draft Privacy Legislation

How can the Ontario government simplify the draft privacy legislation and continue to have it apply to all sectors, including the health sector?

The combining of general rules with health-specific rules for privacy protection does make for a complex piece of legislation. Nonetheless, the IPC supports the government in its desire to create a single comprehensive piece of privacy legislation.

Much of the complexity of the draft legislation is caused by problems with the drafting – difficult and ambiguous language, inconsistencies, redundancies and duplication. This is not a trivial matter. In fact, the IPC believes it cannot overstate the importance of the need to address these issues. If individuals and organizations cannot readily understand their rights and responsibilities, the purpose of the legislation is not served.

Below are examples of the types of problems the IPC noted throughout the draft legislation. The concerns identified here relate solely to the drafting, not to the content of the provisions – any substantive issues the IPC has about specific sections are identified elsewhere in this submission.

Complex Drafting

While acknowledging the need for precise legislative language, the IPC believes the entire draft legislation would benefit greatly from a plain language review. For example, section 56(1) is a critical section relating to the individual's right of access. The introductory language of that section reads:

> Subject to this Part, an individual is entitled, in accordance with this Part, to access to personal information about the individual that is not personal health information and that is in the custody or under the control of an organization that is not a health information custodian, including information on its use and disclosure, unless, ….

The IPC questions how easy this section is to understand, particularly with the inclusion of both "subject to this Part" and "in accordance with this Part." The government must recognize this legislation will have a broad range of users, including the general public unaccustomed to the specificity and complexity of legislative language.

Cross-referencing is another example of how the current drafting style actually increases the reader's confusion. It is understood that, at times, it is necessary to reference other sections in the legislation. However, the overuse of this technique in this draft legislation forces the reader to continually flip from one section to another, and then try to determine how the sections relate. For example

section 44 (Disclosures related to this or other Acts) commences "Subject to section 41…." Turning to section 41 (Disclosures for proceedings), the reader discovers it starts "Subject to section 42…." Section 42 (Disclosure of personal mental health information) then goes on for three pages. The drafting makes the determination of what disclosures are permitted relative to this or other Acts very difficult.

Inconsistencies

One of the most basic and serious problems created by inconsistent language is not being able to quickly understand who is being referred to in a provision. Section 2 of the draft legislation defines "individual" and "organization." The definition of organization includes reference to a "person" because sometimes responsibilities of an organization need to be discharged by a person (e.g., a sole proprietor). Confusion arises when sections reference a "person" who is to function in a manner other than an organization, but not in a manner consistent with the definition of an individual – meaning the individual to whom the personal information relates.

Sometimes the context makes it clear whether the reference to a person relates to an individual or organization. For example, section 80(1)(c) permits specifying in the regulations "persons or class of persons" to be exempted from the definition of health information custodians. Since the definition of organization explicitly includes custodians, it is clear in this section the reference to a person may be read as meaning organization.

However, sometimes the context does not make it clear who is being referenced. For example, section 80(2) permits regulations to be applied generally or specifically to any person or class of person. Given that some of the regulation provisions relate to responsibilities of organizations and some to rights of individuals, it is not clear if section 80(2) relates to one or the other or both.

This problem may have arisen because sections from Bill 159, which defined a person to mean "an individual, corporation, partnership, association or other entity" appear to have been cut and pasted into this draft legislation. The IPC stresses the need for a careful and thorough edit of the entire legislation in order to eliminate this problem. Appendix A identifies other examples of specific wording inconsistencies, along with the IPC's recommended changes.

Ambiguities

One of the clearest examples of ambiguity, and its significant impact on the interpretation of the legislation, arises with the consent provision, which states:

> 8. (1) If this Act requires the consent of an individual to the collection, use or disclosure of personal information, the consent may be express or implied, except that the following consents must be express:

1. A consent to the collection of personal health information by an organization that is not a health information custodian.

2. A consent to the collection, use or disclosure of genetic information.

3. A consent that this Act provides must be express, and not implied.

The IPC finds the wording of clause 3 obscure because it seems to be saying that consent must be express when the Act says it must be express. But to the IPC's knowledge, there are no provisions in the draft legislation that specify express consent outside of the circumstances noted in clauses 1 and 2.

In the February 5, 2002 issue of *PrivacyScan*, Murray Long, editor, interpreted section 8(1)3 to mean, "where the *Act* specifies that consent is explicitly required, this consent must be express." This interpretation has significant implications for organizations engaging in fundraising and marketing activities.

The ambiguity of the consent requirements is fostered by the fact that the exemptions from consent identify situations where one could reasonably expect implicit consent to be applicable. For example, if during the provision of health care, implied consent may be appropriate, why is it necessary to explicitly identify such a situation as an exemption from consent (section 34(b))? The principle of consent still applies, it just may not be necessary to obtain express consent. By attempting to define every contingency, the drafting actually gives the impression that the use of implied consent is not permitted.

The consent provisions are amongst the most pivotal of the draft legislation. Therefore, the drafting must be clarified so the appropriate and reasonable application of both express and implied consent, including the use of opt-in and opt-out for marketing purposes, may be clearly understood. At a presentation to external stakeholders on February 13, 2002, MCBS acknowledged the confusion about consent and indicated that it will be working to clarify these provisions. The IPC is very supportive of this undertaking.

We would like to stress the pressing need for the government to clarify if and when, under the draft legislation, organizations will be permitted to use opt-out when using and disclosing personal information for marketing purposes. In particular, an explanation of how opt-out fits within the draft legislation's definitions of express and implied consent is essential. If the intention of the government is to prohibit this marketing practice, we believe there may be significant harmonization problems regarding the consent principles of PIPEDA. Under Principle 4.3, the federal legislation clearly recognizes that the form of consent may vary according to the sensitivity of the information and the reasonable expectation of the individual. It also includes a checkoff box (opt-out) as an example of a form of consent (4.3.7). It is unclear to us why Ontario would wish to create a standard

distinct from the rest of Canada. Also, we question if individuals would reasonably expect the same standard of consent for genetic information as for personal information used and disclosed for marketing purposes.

We also encourage MCBS to clarify when consent needs to be sought for the use and disclosure of personal information already in the custody and control of organizations, after the legislation comes into force.

Another problem with the current drafting is that sometimes provisions are so broadly worded the IPC is unsure exactly what they mean. One of the most significant examples is section 80(4), which states:

> A regulation may adopt by reference, in whole or in part, with the changes that the Lieutenant Governor in Council considers necessary, any code, formula, standard, guideline, protocol or procedure, and may require compliance with any code, formula, standard, guideline protocol or procedure so adopted.

The purpose of this section is not at all clear. If it is designed to allow the government to approve technical standards (e.g., a certain type of encryption), in principle, the IPC does not object. The ambiguity arises with the use of the term "code." This word has a precise meaning when associated with privacy legislation – it is a "term of art" in this context. For example, in the New Zealand privacy legislation, a code is, in effect, a separate legal regime for a particular industry. It can stand in the place of legislation, and can even lower the privacy standards. The IPC would have grave concerns about the adoption of this type of code in the manner authorized under section 80(4). The intent of this section should be made clear.

Redundancies

There are many provisions in the draft legislation stipulating matters that seem to be implicit, particularly in the provisions relating to exemptions to consent. For example, sections 37(1)(f) and 44(i) give organizations the discretion to disclose personal information without consent for the "purpose of having a legally authorized person or body carry out legally authorized activities to administer or enforce" a law. The IPC wonders why, then, sections 37(1)(g) and 44(e) are necessary? Are not the Public Guardian and Trustee and the Children's Aid Society legally authorized bodies carrying out legally authorized activities? The inclusion of these types of sections may unnecessarily add to the length and complexity of the draft legislation.

Throughout this submission, the IPC has identified examples where it may be reasonably argued the sections are implicit, or may be subsumed under other broader provisions. Should the government want to simplify the draft legislation, consideration should be given to eliminating these redundant sections.

Duplication

As noted above, the IPC supports the integration of privacy protections for the broader private sector and the health sector into a single piece of legislation. However, the draft legislation currently reads as if the sections relating to health have been grafted onto private sector legislation. Significant work needs to be done to simplify, clarify and more fully integrate the two sets of privacy protection rules.

The complexity of the draft legislation is created by having different provisions applying selectively to:

1. health information custodians dealing with personal health information;
2. health information custodians dealing with other forms of personal information;
3. organizations other than custodians dealing with personal health information; and
4. organizations other than custodians dealing with other forms of personal information.

Sometimes these are necessary distinctions. However, sometimes they are not, and then they unnecessarily add to the length and complexity of the draft legislation. The separate access provisions for health information custodians is the most obvious example of duplication.

It is confusing to make a distinction between organizations and custodians when no special rules apply to custodians. If the same provision applies to all types of organizations and to all types of personal information, separating out health information custodians creates unnecessary duplication. This is a particular problem under the exemptions to consent provisions. By duplicating general application provisions in sections relating exclusively to custodians, the drafting actually creates the false impression that custodians are required to follow only those sections that expressly reference them. In fact, custodians also are required to follow the general requirements, particularly in the context of their employee records.

It would be clearer to all parties if the provisions common to all organizations are grouped together. Only those necessary exemptions or additional rules relating to personal health information or custodians need be identified in separate sections.

The distinction between custodians and other organizations could be further reduced if some of the custodian-specific provisions are applied to all organizations. For example, sections 36(2), 49(1)(c), 52(4), 62(13)(b), and 64(11), which all currently apply only to custodians, should apply to all organizations.

For all the reasons noted above, the IPC strongly encourages MCBS to undertake a detailed review of the wording and structure of the draft legislation. The IPC will gladly assist in this endeavour. Existing ambiguities, duplication, and confusion will make implementation and administration of the legislation difficult and time-consuming. Clear and comprehensible language is essential in order for the public and organizations to understand their rights and responsibilities.

2. Right Balance

Has MCBS found the right balance between individual privacy protection and the reasonable needs of organizations in Ontario? How might the legislation be improved in this respect?

Experience in other jurisdictions clearly demonstrates that the individual's need for privacy and the organization's need to collect, use and disclose personal information do not necessarily have to be viewed as mutually exclusive – or being at the opposite ends of a scale. The IPC argues that privacy is actually an important business need in terms of customer service.

While acknowledging that we are in a more informed position to comment on appropriate privacy protections than on the needs of organizations, we believe, with necessary changes, the draft legislation can find the right balance between these considerations.

By using the 10 principles of the Canadian Standards Association's *Model Code for the Protection of Personal Information* as the foundation of this draft legislation, the government has gone a long way toward putting in place appropriate and effective privacy protections. For the most part, the draft legislation covers the principles in an appropriate manner. Appendix B outlines the IPC's suggestions for enhancing the privacy protectiveness of a number of provisions not addressed elsewhere in our submission.

The remainder of this submission is devoted to outlining ways in which the IPC believes the privacy protections of the draft legislation can be improved. Our comments throughout follow a number of general themes:

- enhancing the ability of individuals to exercise their rights;
- narrowing exemptions to consent;
- strengthening oversight; and
- reducing the scope of the regulations.

Definitions (section 2, page 15)

Do the definitions provided here help you to interpret the draft bill?

Are there any definitions that require further clarification? For example, are the definitions of "health information custodian," "professional identity information," and "personal information" clear to you?

Are any definitions missing?

While the 44 definitions in the draft legislation far exceed the number in any other Canadian private sector or health privacy legislation, the IPC does not, in principle, object to the inclusion of anything that enhances the reader's ability to understand and interpret the legislation.

The IPC is concerned that the current wording of the definition of "disclose" may be interpreted to mean the draft legislation does not regulate disclosure to individuals acting in a personal non-commercial capacity. We believe the definition should be amended to say:

> "disclose", in relation to personal information in the custody or under the control of an organization, means to make the information available to an organization that is not an agent of the disclosing organization **or to an individual acting in a personal non-commercial capacity**…."

The ability to prescribe registries and repositories should be removed from clause 7 of the definition of health information custodian. In addition, specific criteria for registries and repositories should be added to the definition in order to clarify and rationalize what organizations are covered. This would ensure consistent application of the draft legislation.

It is our understanding that employee human resources records held by organizations subject to the legislation are to be covered. We are concerned this intent is not clear in the definitions of types of information excluded from the definition of personal information. Specifically, we think the definition of professional identity information is not clear. First off, the IPC thinks the term "professional identity information" is confusing and recommends changing it to "professional information." Secondly, while we think the exclusion of professional activities from the definition of personal information is essential in order to enhance professional accountability, we are concerned that the inclusion of the phrase, "the manner in which the individual carries out those responsibilities," could be interpreted to include human resource matters, such as an employee's performance appraisals. Therefore, the IPC recommends the government re-work this definition to make it clear employee human resources records are covered by the draft legislation.

Non-Application of Act (section 7, page 19)

As a general principle, the scope of section 7 should be narrowed. For example, "Anything in the *Trillium Gift of Life Network Act*" (section 7(3)4) should not prevail over privacy legislation. That provision should be removed or narrowed by adding a reference to specific sections in that statute.

The temporary measure under section 7(1)(j) speaks to the larger issue of the difficulty of making an accurate and complete assessment of all other legislation potentially affected by the privacy legislation, prior to its introduction. When introduced, FIPPA included a provision requiring a committee of the Legislative Assembly to undertake a comprehensive review of all confidentiality provisions to determine the issue of prevalence. The government should give consideration to such a provision for the *Privacy of Personal Information Act, 2002*.

The IPC believes section 7(1)(k) is unreasonable and inappropriate, and strongly recommends its removal. Privacy legislation should not include a provision that permits anything and everything covered by that legislation to be excluded by regulation.

MCBS would like to seek a balanced approach to the freedom of speech and the protection of privacy. We are interested in hearing your views on this matter.

There are legitimate purposes for the collection, use and disclosure of personal information where the application of privacy legislation is unworkable, unnecessary, or inappropriate. Personal use of information is the most obvious example. The collection, use and disclosure of personal information for artistic, journalistic or literary purposes is another. Some people may wonder why someone should be able to use or disclose their personal health information without their consent just because that person is writing a book or creating a work of art. Should not the privacy of the individual be paramount in these circumstances?

The *Canadian Charter of Rights and Freedoms* guarantees freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication (section 2(b)). Journalistic freedom is essential to a democratic society, such as Canada. It also must be recognized that freedom of expression is not just limited to the press – it includes a wide range of artistic and other endeavours by all manner of people.

These fundamental freedoms must be protected and, after considering alternatives, the IPC concludes the approach taken in the draft legislation is reasonable. Section 7(1)(b) of the draft legislation is similar in intent and language to section 4(2)(c) of PIPEDA. To take a different approach, when the net result is essentially the same, would not serve a useful purpose.

Although recognizing the legitimate need for this exclusion from the legislation, the IPC remains concerned about how this "carve out" will be applied and by whom. Care must be taken to ensure this provision is not abused. For example, there is a need to bring focus to the determination of who may be appropriately considered to be engaging in journalistic activities. Over time, the IPC and the courts will need to address this critical issue.

In the context of this exclusion, organizations also will need to understand the condition "and for no other purpose" in section 7(1)(b) means personal information collected for artistic, journalistic or literary purposes may not be used or disclosed for other purposes without the consent of the individual to whom the information relates. Another critical point is the fact that the provision relates to the personal information, and not to the organization. This means that the information only, and not the organization, is excluded from the legislation. For example, a newspaper's employee and subscriber records would be covered.

As the identified oversight body, the IPC will be in a position to help refine the interpretation of this section, and to help educate organizations about its meaning and appropriate application.

Consent – Special Rules for Health Sector (section 8, page 22)

Do you support having special rules for personal health information in the hands of organizations that are not health information custodians?

Do you think these rules, together with the general rules provide sufficient protection for personal health information in a non-health care setting? If further protections are required, what should they be?

We agree that express consent should be required for collection of personal health information by an organization that is not a health information custodian (section 8(1)1).

For the most part, the general rules are sufficient for protecting personal health information in the non-health care setting. However, the addition of specific provisions to narrow the disclosure of this information without consent (e.g., sections 37(2) and (3)) are appropriate. The IPC supports the inclusion of special rules for the protection of personal health information only when they are necessary and useful.

The one area of concern for the IPC relates to the use and disclosure of personal health information for research purposes by organizations other than health information custodians (section 33(1)(e)). We discuss this specific issue later in our submission.

Withdrawal of Consent (section 12, page 27)

Are these exceptions to the right to withdraw consent reasonable?

Are there other circumstances where individuals should not be able to withdraw their consent?

One of the essential components of true consent is the ability to withdraw it. If someone voluntarily consents to the collection, use and disclosure of his or her personal information, the individual should be able to change his or her mind and withdraw that consent. However, there are circumstances when it should not be permissible for the individual to withdraw consent. The individual's understanding of these restrictions on the right to withdraw consent is a critical part of informed consent as defined by section 8(4)(b).

The IPC's major concern relates to the government's ability to add further restrictions to the right to withdraw consent by regulation under section 12(1)(f). It is not appropriate for privacy legislation to permit the government, without public consultation, to restrict the rights of the individual. Accordingly, section 12(1)(f) should be removed. Additional exceptions to the right to withdraw consent should be specified in the legislation.

In the context of health research, the IPC does not think it appropriate to entirely prohibit the withdrawal of consent. While recognizing the challenges, we would like to see section 12(1)(e) amended to permit the individual to withdraw consent for future uses, if reasonably practical.

Substitute Decision-Makers (sections 13-18, page 29)

Are these provisions appropriate in the context of privacy protection for personal health information?

Should these rules for substitute decision-makers regarding personal health information be streamlined with the general rules for personal information?

The sections regarding the appointment of substitute decision-makers are amongst the most confusing of the draft legislation. The IPC supports the inclusion of provisions to address situations where individuals are not capable of providing consent for the collection, use and disclosure of their personal information. But we also think it is important to remember that the consent is relative to the handling of personal information, not to medical treatment.

By way of background, Principle 4.3.6 of PIPEDA indicates that consent may be given by "an authorized representative (such as a legal guardian or a person having power of attorney)." Section 104 of Alberta's *Health Information Act* outlines when it is permissible for an individual's rights to be exercised by other authorized persons. The same sort of provision may be found in section 60 of Manitoba's *Personal Health Information Act* and section 56 of Saskatchewan's *Health Information Protection Act*.

While recognizing the need to adopt an Ontario-specific solution to this issue, and the fact that we are not bound by the actions of others, the IPC questions the need for the inclusion of six pages of detailed requirements. This is one of the times when we do not understand why custodians need to have everything identified in the privacy legislation, when other types of organizations do not.

Section 10(1)2i already recognizes that, if an individual is incapable of consenting, a person "who is authorized at law to consent on behalf of the individual" may do so. For custodians, a determination of authority could be made under the appropriate statute (e.g., the *Health Care Consent Act* and the *Substitute Decisions Act*), without needing to include specific provisions in the legislation. If necessary, a provision could be added to make it clear that if a person is authorized to consent to treatment, that person also is authorized to consent to collection, use and disclosure of personal health information by custodians in limited and appropriate circumstances.

Representatives from the Ontario Medical Association (OMA) raised an additional issue with the IPC about the current drafting of the substitute decision-making provisions. The OMA's concern was that while these provisions closely parallel those in other legislation governing substitute decision-making in the health sector, there are a number of variations that may not be readily identifiable. These variations may cause confusion for health care providers and patients. The OMA also noted that proceedings under the draft legislation are not linked to those proceedings to

determine capacity to consent to treatment under other legislation. This could lead to duplicate proceedings – one for consent to treatment, and another for consent to collect, use and disclose personal health information. Instead of attempting to make changes to existing practices by including similar but different requirements in privacy legislation, the OMA thought it more reasonable to make consequential amendments to the appropriate statutes.

Should there ultimately be a consensus amongst health stakeholders that it is absolutely necessary to have these provisions in the legislation, rather than included by reference, the IPC defers to their expertise, but recommends moving them to the regulations.

Consent for Collecting Health Information in the Health Sector (section 19, pages 35-36)

Your views on the options below or alternative recommendations would be valued.

(i) CONSENT FORM Require health organizations to obtain express consent from patients, upon their first visit, through a signed form.…

(ii) NOTICE FORM Require health organizations to provide a notice to individuals about the purposes for which their personal health information is being collected.…

(iii) CONSENT IMPLIED IN THE CONSENT TO TREATMENT Under this approach, it would be assumed that presenting oneself for treatment is equivalent to consent to the collection, use and disclosure of personal health information for the purpose of receiving treatment.…

The purposes section (section 1) of the draft legislation is the foundation upon which all other provisions rest. The privacy protections afforded by this legislation may be effective only with the recognition of, and respect for, individuals' entitlement to provide or withhold their consent, and to be informed of how their personal information is collected, used and disclosed. Without these essential components, privacy is not possible.

Therefore, it is undesirable for the elements of consent and notice to be eliminated completely from the collection, use and disclosure of personal health information by the health sector. The highly sensitive nature of this information absolutely necessitates consent being sought, when appropriate.

As presented in the consultation draft, option (i) references express consent, option (ii) requires notice of purpose, and option (iii) acknowledges the use of implied consent in the context of the provision of health care. The IPC believes that it is an artificial distinction to treat these options as mutually exclusive. Express consent, notice and implied consent all have appropriate applications for the collection, use and disclosure of personal health information within the health care system. Discussing each option in reverse order, the IPC acknowledges that the challenge is determining which alternative is reasonable and appropriate to which circumstance.

Option (iii) Consent Implied in the Consent to Treatment

For many activities relating to the provision of health care, implied consent for the collection, use and disclosure of personal health information by health organizations may be appropriate. For example, the IPC does not believe a lab needs to get the individual's consent in order to disclose the results of a test to the individual's physician, who requested the test be conducted. That disclosure is implied when the patient agrees to the test.

In order to fulfil this one purpose – the provision of health care – we do not think that it is necessary to obtain express consent for every collection, use and disclosure. However, we would like to stress that the provision of health care should be narrowly defined and does not include uses and disclosures for purposes across the health care system that would not be reasonably obvious to the individual. Also, consent may be implied only where the individual has not expressly made their wishes known. For example, as will be discussed later, under section 38(1)(a), the IPC is recommending a modified lock box.

However, the IPC does not support requiring express consent from the individual to collect, use or disclose their personal health information for all purposes not related to the provision of health care, as indicated in the explanation of Option (iii). We do not think this is a realistic or feasible option.

Option (ii) Notice Form

It is important to recognize that the consent requirements for say, video rentals or purchasing an insurance policy, do not literally translate to the health sector. In Ontario, the health care system is publicly funded. As such, it functions much more like a government system than a private enterprise. For the most part, it is not possible for individuals to take their business elsewhere. At the same time, a health care provider may not refuse to provide treatment. In addition, there is a legislative framework in which the health care system must function, including the mandatory collection, use and disclosure of some personal health information in prescribed circumstances.

To ask for consent when it is not meaningful, and does not meet the criteria of informed consent, as defined by section 8(4), is not appropriate. For example, it is not appropriate to ask for consent for a required disclosure to the Chief Medical Officer of Health (section 39(1)(a)). It is for this reason that the IPC believes there is a very necessary and useful place for notice within the health care system. One of the overarching purposes, as set out in section 1(a)(ii), is that "individuals are entitled to be given information sufficient to know how their personal information is to be collected, used and disclosed." This information enables the individual to make informed decisions and to take action, if necessary. In order to facilitate this, the IPC argues for an expansion of the notice provisions in the exemptions to consent related to the health care system, as discussed later in this submission.

It is both reasonable and appropriate for custodians to inform individuals of the collections, uses and disclosures of their personal health information required by law, and when their personal health information is used and disclosed for broader purposes across the health system. They also should inform individuals that their express consent should be sought for collections, uses and disclosures of their personal health information by other organizations (e.g., employers or insurance companies) for other purposes, as indicated under Option (ii).

Although consent may not be appropriate in certain circumstances, this does not mean that the personal health information is not protected by other means. The IPC is pleased with restrictions on the collection, use and disclosure of personal health information under sections 20(2) and 21. Further, as will be discussed later in this submission, the IPC recommends narrowing of legislative requirements for exemptions to consent, and broadening the scope of the health data institute in order to enhance privacy.

The IPC does not support the conclusion under Option (ii) that: "In other words, the notice would replace the consent requirement within the health system." Not only does this not recognize the importance of implied consent in the context of the provision of health care, it fails to recognize that there is a very real need for express consent for non-routine or unrelated purposes even within the health system. A health care provider should not be permitted to use or disclose personal health information for purposes wholly unrelated to the provision of health care without requiring express consent.

Option (i) Consent Form

Although called "Consent Form," this option is really a variation on notice. It just requires a signed acknowledgement of notice. In our view, it is misleading to say this is express consent because individuals are not given any real choice about the collection, use and disclosure of their personal health information. We are also uncertain of the benefit of having a signed acknowledgement of notice.

Having said that, the IPC believes there are times when express consent may be appropriate within the health care system. The modified lock box and secondary uses and disclosures unrelated to the purposes for which the information is collected, as noted above, are two examples of when express consent should be required.

To the maximum extent possible, the IPC supports enhancing the transparency of the health care system in terms of collection, use and disclosure of personal health information, and providing individuals with the information and opportunity to exercise their rights under this legislation. However, we also recognize that, in a publicly funded health care system, privacy may not be the sole value to consider. There are larger societal benefits to having an efficient and effective health care system. The challenge is to find the appropriate balance between the protection of the individual's privacy and the need to use personal health information in order to deliver quality health care.

Express and implied consent, as well as notice, have their legitimate uses within the health care system. Therefore, the IPC cannot definitively support one option over the others. As presented in the consultation draft, none are clearly applicable in all circumstances. Implied consent may be appropriate in the context of the provision of health care, when express consent is absent; notice

is essential for individuals to understand how their personal health information is used and disclosed within the health sector and beyond; and express consent is the only reasonable option for situations when an unrelated use or disclosure is being contemplated.

While this makes it difficult for health organizations to clearly understand which option is reasonable or appropriate to any given situation, the IPC believes that it is essential to recognize that elements from each of the three options have merit. This lack of a simple solution necessitates the legislation be drafted to accommodate express and implied consent, as well as notice. It also necessitates that guidance and support be given to the health sector in order for custodians and others to understand how and when to apply the options in the most appropriate manner. As the identified oversight body, the IPC believes it will be able to play a key role in this regard.

Despite the operational difficulties, the principles of consent and notice must be applied to the health sector. The contentious issues are the allocation of responsibility (i.e., who tells what to whom) and the mechanism (e.g., standardized forms, pamphlets or notice posters).

No one wants patients to be faced with pages and pages of densely written text outlining every potential purpose for which their personal health information may be used. Further, no one wants health care providers to be pulled away from the provision of valuable health services in order to explain a use of personal health information by another health organization over which they have no control.

Although the health care providers are the point of contact with the individual, this does not necessarily mean they should be responsible for explaining every purpose for which the patient's information may be used or disclosed. Clear and concise material should be provided to patients at their initial contact with their health care provider. This material needs to explain how their health information will be used and by whom, when their consent for the provision of health care will be implied, when express consent will be required, and who to contact should they have questions.

The IPC supports the careful examination of these operational issues with health stakeholders, including patient advocates. In order to reduce the administrative burden on health care providers, the IPC favours standardized consent and notice forms (where appropriate), and will be pleased to work with the government and stakeholders to develop mechanisms that are meaningful, useful and effective.

Fundraising (section 26, page 38)

In your opinion, should there be any exemptions or modifications to the consent requirement when collecting, using or disclosing personal information for fundraising purposes? Should the … rules for fundraising in the health sector remain as proposed?

The IPC agrees with the inclusion of a general prohibition against using personal information for fundraising activities without the consent of the individual (section 26). As was noted earlier about marketing, we request clarification as to whether opt-out will be permitted under the draft legislation for fundraising beyond the health sector.

In certain high stress or emotional situations, like those surrounding the provision of health care, individuals may not be in a state of mind to express their true wishes concerning the use and disclosure of their personal information for fundraising purposes. Therefore, the IPC supports the proposed health sector regulation, particularly the requirements restricting fundraising activities to those related to the organization's operation without reference to the health care provided. The regulation should make it clear that it does not apply to the broader health sector, but rather only to health information custodians that are facilities, such as a hospital or home for special care.

Exemptions to Consent for Collection, Use and Disclosure
(sections 33-48, pages 40-41)

In your opinion, are these exemptions reasonable?

Do these exemptions strike the right balance between protecting an individual's right to control how their personal information is used with the needs of organizations to use personal information for purposes that are reasonable and appropriate? For example, do you think it is reasonable to allow organizations to collect personal information without consent or without a warrant to investigate or to determine whether to investigate a possible breach of a contract or law in Canada?

Please comment on the specific exemptions of importance to you.

As a fundamental principle, the IPC recommends minimizing exemptions to consent. In our opinion, the current wording of the exemptions has yet to strike the right balance between the individual's privacy rights and the needs of the organization.

Below are the IPC's concerns and questions regarding the exemptions to consent for collection, use and disclosure. To simplify presentation and to facilitate future discussions with the government about these issues, our response is organized into recurring themes: reasonableness, notice (where appropriate), and drafting issues.

Collection without Consent

Reasonableness of Exemptions

The scope of section 33(1)(i) is not reasonable. Just because a collection is permitted by a law, an organization's obligation to obtain consent is not negated. This exemption should be narrowed by removing "authorized." A legislative requirement to collect should be necessary before this exemption to consent may be applied. Similar concerns exist for sections 34(a) and (c). It is not sufficient for a statute to permit a custodian to indirectly collect personal health information in order to be exempted from the consent requirement. The application of section 34(a) should be narrowed by replacing "authorized" with "required." Also, just because an organization is permitted to disclose personal health information does not mean a custodian should have the right to collect it without consent. The removal of "authorized" in section 34(c) is also recommended.

The scope of section 33(2) needs to be clarified. As currently worded, this exemption could be read to cover negotiations or business transactions with an individual. A non-disclosure obligation does not justify collection without consent in this context. If the government's intent is to cover business-

to-business negotiations and transactions, the exemption has to make that clear. The relationship between this provision and section 33(1)(g) also should be clarified.

It is reasonable for an organization to collect personal information without consent or a warrant, in limited circumstances. It is important to remember this draft legislation does not authorize collection by law enforcement agencies. They are covered by Ontario's public sector freedom of information and privacy legislation. The one improvement the IPC would like in this area is the reasonableness test under section 33(1)(b) to be included in section 34(d) as well.

Notice Requirements

The provision of notice for collections without consent enhances the transparency of the process for the individuals to whom the personal information relates, and enables them to take action, if necessary. Accordingly, the IPC recommends expanding the notice requirements to include sections 33(1)(g), 33(1)(i), and 33(2).

In the context of health information custodians and the collection of personal health information, the IPC is concerned because there are no notice requirements. This is an instance when special rules for custodians are not appropriate as they do not enhance privacy. To be consistent with the general provisions, notice should be required for sections 34(a), (b), (c) and (e). In addition, sections 33 and 34 could be streamlined by having only one notice provision per section, with appropriate references or exclusions.

Drafting Issues

The wording of section 33(1)(b)1 broadens the scope of this exemption beyond what is contemplated by PIPEDA. We would like to know what additional circumstances the Ontario government is trying to cover with the phrase "including the common law." In addition, we are confused by the different wording used in section 34(d). Are the two sections meant to accomplish the same thing? If so, why the different wording, and why is common law not included in section 34(d)? The wording of section 33(1)(b)1, as it relates to rules and other instruments, also may need to be changed. It seems more logical for "or" rather than "and" to be used, but the IPC requests clarification from the government on the rationale for the current wording.

Below are other questions regarding issues arising from the drafting:

- Why is section 33(1)(f) necessary if section 33(1)(i) is intended to cover all circumstances and all law?

- Why are sections 34(d) and (e) worded differently than sections 33(1)(b)1 and 33(1)(h)1 respectively? Are the purposes the same or different?

Use without Consent

Reasonableness of Exemptions

The IPC strongly objects to section 35(d), which permits organizations to use personal information without consent for any purpose prescribed in the regulations. Such an exemption is not reasonable or appropriate because it permits an end-run of the consent requirements, without any public scrutiny or accountability. All necessary exemptions to consent should be defined in the legislation.

For all the reasons noted above regarding collection without consent, the IPC recommends the removal of "authorized" from sections 36(1)(b) and (k).

Under section 36(1)(c), the IPC questions the need to use any personal information, particularly personal health information, for planning of programs or services and allocating resources. A full explanation from the government on why these purposes cannot be fulfilled with de-identified information is requested. We also would like to know why this section does not have to follow the process set out in section 47 involving a review by a technical committee and the use of a health data institute.

Drafting Issues

Below are additional questions about the drafting of the use without consent exemptions:

- Why is section 36(1)(e) necessary? The definition of an agent is a person who "acts for or on behalf of the organization" so why does this distinction for use need to be made? If it is necessary, why is it not necessary for organizations other than health information custodians? Having this exemption to consent only for custodian gives the impression that consent is required for use by an agent in other sectors. Is this the government's intent?
- What is an example of what section 36(1)(f) covers that is not already covered by section 36(1)(e)? If the agent is not performing a duty on behalf of the custodian, then why would consent for use of personal health information for educative purposes not be required?
- Is section 36(1)(h) not implicit in section 34(e)? If a custodian is authorized to collect personal health information for the purposes of a proceeding, why is specific authority needed to use that information for the same purpose in a proceeding? The need for this provision is further questioned because section 36(1)(a) permits use of personal health information to fulfil the purposes for which it was collected.
- Why is section 36(1)(i) necessary given the definition of implied consent under section 8(5)? How would it not be "reasonably obvious" to individuals that a custodian would need to use and disclose their personal health information (e.g., health numbers) in order to get paid for the services provided to the individuals?

Disclosure without Consent

Reasonableness of Exemptions

It is unreasonable for personal health information to be disclosed without consent in order to administer, investigate or enforce a by-law. The references to by-laws should be removed from sections 37(1)(e) and (f), as well as section 44(i). If absolutely necessary, the requirement for by-laws under section 37(1)(e) and (f) should be moved to section 37(2) so disclosure of personal health information is explicitly excluded.

The wording of section 37(1)(j) should be narrowed so it is clear that this exemption does not apply to any and all business transactions. The use of the word "function" rather than "purpose" is problematic. Disclosure of personal information should only be permitted if the receiving party is statutorily or contractually bound not to use the information for any purpose other than that for which it was disclosed. That obligation should also extend beyond maintaining confidentiality to include all appropriate protections for privacy (e.g., security and accuracy). In addition, the timing of this exemption should be clarified in a manner similar to section 37(3)(b).

Following our comments related to the need for consent in the health sector, section 38(1)(a) should be amended to indicate that disclosure to another custodian should only be permitted in circumstances where the individual has not instructed the custodian to the contrary. This would create a type of a lock box.

We recognize that the inclusion of the lock box could, in some cases, allow individuals to withhold key personal health information that may be critical to their care and treatment. However, it should be noted that providing individuals with the right to prevent disclosures of all or part of their record of personal health information does not necessarily mean that this information could never be shared for health care purposes. It simply means that the custodian's judgment would not be the sole consideration. Information would not automatically flow freely among those persons who are directly or indirectly involved in the individual's health care, without any involvement on the part of the individual. Instead, the individual would have to be consulted and consent obtained, on a case-by-case basis, before the custodian could disclose the locked part of the record for health care purposes. In addition, if an individual does not expressly choose to utilize the lock box, it may be appropriate to imply consent for disclosures relative to the provision of health care.

Health information legislation in Manitoba, which has been in force for several years, contains a lock box provision whereby individuals can prevent their personal health information from being shared among health information custodians without their consent. Alberta's and Saskatchewan's health information legislation provide individuals with a means of prohibiting the transmission of their personal health information over electronic networks. In the absence of the lock box or any means for individuals to prevent their personal health information from being made available over computerized networks, Ontario's legislation will not provide the same standard of privacy protection provided in other jurisdictions in Canada.

Section 38(2) should make it explicit that the facility should consult with known family members or friends, if the individual is incapacitated, before disclosing the personal information under this exemption.

The IPC also thinks section 38(3) should be amended. While it may be appropriate to inform a person of the death of another individual, it is not always appropriate to inform him or her of the "circumstances of the individual's death." We would like further discretion built into this provision to permit disclosure of the circumstances surrounding the death only when it is reasonable to do so.

Under section 39(1)(e)(i), registries and repositories should not be able to circumvent, by regulation or any other means, the rigorous review process for research required by section 45. This is an example of where the rules governing a particular use of personal health information should apply to all types of organizations.

Disclosure of personal health information without consent for the purposes of planning or evaluating ambulance services, as authorized under sections 39(3) and (4), is inappropriate. This exemption should be removed in its entirety. These sections do not relate to the provision of emergency services to individuals, but rather to management issues. On the face of it, it seems unreasonable to require the disclosure of personal health information in order to fulfil these purposes. The government needs to clearly explain why de-identified information is not sufficient to fulfil these purposes. It is particularly confusing given that a health data institute has been set up under section 47 because the Ministry of Health and Long-Term Care (MOHLTC) recognizes that de-identified information may be all that is necessary to fulfil the purposes of management, evaluation, monitoring, allocation of resources, and planning of the health system. Why are ambulance services different?

As argued for other exemptions, disclosure without consent should not be permitted simply because a statute permits such a disclosure. Accordingly, "authorized" should be removed from section 44(h), necessitating a legislative requirement before disclosure of personal health information without consent is possible under this provision.

As currently worded, section 44(i) is unreasonable. This exemption could be read to cover anything and everything, and completely negate the consent requirements. Further, the discretion to disclose personal health information may be at odds with a custodian's professional responsibilities (e.g., doctors may be required to insist on a warrant before disclosing personal health information to the police). A meaningful threshold should be added. The government has recognized the need for such a threshold elsewhere (e.g., section 19(8) of the *Remedies for Organized Crime and Other Unlawful Activities Act, 2001* prohibits the disclosure of personal health information without a court order).

Notice Requirements

The IPC recommends the expansion of notice provisions relating to disclosures without consent. Specifically, there should be notice requirements for sections 37(1)(j), 38(1)(a) and 38(1)(b) (if these provisions remain part of the exemptions from consent), 39(1)(a) and (b), 39(1)(c) (when reasonably practical, e.g., where only four files were reviewed), 39(1)(e), and section 40 (when reasonably practical).

Drafting Issues

Questions arising from the drafting of the disclosure without consent exemptions are:

- Why are sections 37(1)(g) and 44(e) necessary given the breadth of disclosures permitted under sections 37(1)(f) and 44(i)?
- If section 33(1)(g) gives an organization purchasing a business limited authority to collect personal information without consent as part of that sale, is it necessary to specify the authority for the selling organization to disclose that same personal information to the purchasing company without consent?
- Why is it necessary to determine the date of the death of the individual if it is 150 years after the creation date of the information? Should the two requirements of section 37(1)(i) be either/or?
- What type of transaction is section 37(3)(b) to cover? Does it authorize the disclosure of personal health information to organizations authorized to collect it under section 33(1)(g)? If so, why just personal health information and not all forms of personal information?

Personal Mental Health Information in Proceedings

(section 42, page 52)

Do these provisions reflect an appropriate balance between protecting the privacy of personal mental health information and the requirements of an efficient justice system?

Personal mental health information is of a particularly sensitive nature. The inappropriate disclosure of such information could create significant stigma, trauma and perhaps even hardship for the individual to whom the information relates.

Section 42(2)(m) should be removed. It is not appropriate for personal mental health information to be disclosed without consent to proceedings identified at a later time in accordance with criteria prescribed in the regulations. This eliminates the public consultation and accountability so critical to the protection of this sensitive information. All exemptions to consent regarding the disclosure of personal mental health information should be identified in the legislation.

The intent of sections 42(3) and (4) is unclear on two points. The first relates to the necessity of holding a hearing about potential harm for proceedings that are not public, and where no party to the proceedings would have access to the personal mental health information, such as the IPC's own proceedings.

As currently worded, section 42(4) requires the court or body holding the proceeding to hold a hearing if there is a possibility that disclosure in the proceeding would result in harm. During the course of that hearing, the personal mental health information in question is disclosed to the court or body so it may make a determination of harm. Clearly, the real and justifiable concern is not the potential harm caused by disclosure to the court or other body, but the potential harm caused by disclosure in a public proceeding. Therefore, section 42(4) should exempt those proceedings identified under section 42(2) whose mandate and practice prohibit the disclosure of personal mental health information to the public or any party to the proceedings. To require a hearing when there is no possibility of disclosure in a proceeding seems like a needless delay.

The second unclear area relates to oversight. Is it the intention of the government to make all the proceedings relative to section 42, including the harm hearings, subject to the IPC's oversight? Section 63 permits an individual to complain to the Commissioner about possible contravention of any provision of the legislation. This would include the proceedings under section 42. Traditionally, the courts or other bodies have had the final say on issues of disclosure related to their own proceedings.

Disclosure for Research (section 45, page 57)

Do these provisions achieve the right balance between protecting the privacy of people's health information and the public interest that is served by health research?

Will the rules and obligations be clear to organizations who wish to conduct research in the health sector?

Do these rules provide sufficient transparency, accountability and safeguards in the research process?

The draft legislation incorporates a number of safeguards for the use and disclosure of personal health information, in the custody of health information custodians, for research purposes. Central to the proposed framework is the review and approval of research projects by a research ethics board. The IPC agrees, in general, that this approach provides the right balance between protecting the privacy of personal health information and the public interest served by health research. However, we recommend a number of additions and modifications to section 45 in order to strengthen the safeguards to protect privacy; to clarify the rules and obligations for researchers; and to enhance transparency and accountability in the research review process.

Criteria for assessing whether consent should be required

In assessing whether the research should be permitted without consent, research ethics boards should consider whether it is reasonably practical for the researcher to obtain consent, as well as the purposes for which the personal health information will be used. Specifically, research ethics boards should consider the following questions:

- is it reasonably practical for the researcher to obtain consent;
- will the personal health information be used only for the purpose of linking or matching across time and/or sources;
- will the personal health information be de-identified as soon as the linking or matching procedure has taken place; and
- will the personal identifiers be destroyed or, where the personal identifiers must be retained, will safeguards be put in place to limit access to the personal identifiers once the linking or matching procedure has taken place?

Criteria for assessing whether it is reasonably practical to obtain consent

The Canadian Institutes of Health Research (CIHR), in its *Recommendations for the Interpretation and Application of the Personal Information Protection and Electronic Documents Act (S.C. 2000, c.5) in the Health Research Context*, outlined a number of criteria to be considered when assessing the practicality of obtaining consent. In our view, it would be helpful to the research community if similar criteria are incorporated into Ontario's privacy legislation. Borrowing from the work of CIHR, the IPC recommends research ethics boards consider the following factors when assessing whether it is reasonably practical for the researcher to obtain consent:

- the size of the population involved in the research;
- the proportion of individuals who are likely to have moved or died since the personal health information was originally collected;
- the risk of introducing potential bias into the research, thereby affecting the generalizability and validity of the results;
- the risk of creating additional threats to privacy by having to link personal health information with other personal information in order to contact individuals to seek their consent;
- the risk of inflicting psychological, social or other harm by contacting individuals with particular conditions or in certain circumstances;
- the difficulty of contacting individuals directly when there is no existing or continuing relationship between the organization and the individuals;
- the difficulty of contacting individuals indirectly through public means, such as advertisements and notices; and
- whether the additional resources needed to obtain consent will impose an undue hardship on the organization.

Contacting research participants

The draft legislation requires the researcher to enter into an agreement with the health information custodian in which the researcher agrees, among other things, not to contact the individual to whom the information relates unless the custodian authorizes the researcher in writing. Having the custodian authorize contact does not provide sufficient privacy protection. Such a scheme unnecessarily restricts the individual's control over his or her personal health information. Instead, where the researcher proposes to contact individuals directly or indirectly, the consent of the individual should be obtained by the custodian before disclosure. Alberta's *Health Information Act* and Manitoba's *Personal Health Information Act* both require consent before researchers can contact individuals.

Enhancing transparency in the research ethics review process

Once a research ethics review body has approved the use or disclosure of personal information or personal health information without consent, the legislation should require researchers to inform the IPC of their research, prior to its undertaking. This would be compatible with the requirements under PIPEDA. In addition, to enhance transparency, research ethics boards should be required to provide a summary of all research proposals involving personal information they review, as well as their decisions, in their annual reports mandated under section 45(3).

In your opinion, should different rules apply to research involving personal health information outside of the health sector, or should one set of rules apply to the disclosure of this information for research purposes?

The IPC's preference is for one comprehensive scheme. Under the draft legislation, disclosure of personal health information by a health information custodian requires the approval of a research ethics review board (section 45), while the disclosure of personal information, including personal health information, by all other types of organizations requires the approval of the IPC (section 33(1)(e)). In addition, as noted above, there is no review or approval process prior to registries and repositories obtaining personal health information without consent for research purposes (section 39(1)(e)). The different rules may be confusing and, in some cases, unnecessarily burdensome for the research community.

Most research involving personal information is already subject to review by a research ethics board. Unless the privacy safeguards set out in the draft legislation are incorporated into this existing research review process, some projects will be subject to two approval processes – one by a research ethics board and another by the IPC. All research involving the use or disclosure of personal information should be subject to review by a research ethics board, in accordance with requirements similar to those set out in section 45 (with the additions and modifications suggested above). In addition, the IPC should be notified before the research is undertaken. Approval by the Commissioner should be required only in limited circumstances where it is not possible for the research proposal to be reviewed by a research ethics board.

Disclosures for Analysis of the Health System and to the Minister of Health and Long-Term Care (sections 47 & 48, page 62)

Do these provisions contain sufficient safeguards to protect the privacy of people's health information? We would be interested in your views on this approach.

One of the least privacy protective aspects of Bill 159 was the scope of the disclosures of personal health information without consent that could be directed by the Minister of Health and Long-Term Care. Of particular concern was the exclusion of the directed disclosures from any oversight by the Commissioner, and from the application of the general limiting principles, set out in section 12 of Bill 159.

In our submissions and presentations to the Standing Committee on General Government, the IPC strongly recommended the removal of the directed disclosure provisions from Bill 159. As minimum privacy safeguards, we recommended all directed disclosures be subject to review by the Commissioner and to the general limiting principles, such as the requirement to disclose anonymized or pseudonymized health information, whenever possible.

We are pleased the government has addressed the concerns raised by the IPC and other stakeholders in the draft legislation. The introduction of an intermediary health data institute signals a recognition that, in all but the most exceptional circumstances, de-identified information is sufficient for the MOHLTC to fulfil the purposes of managing, evaluation, monitoring and allocating resources, as well as planning for the health system.

The IPC supports the scope of the technical committee's review, as well as the transparency and accountability built into the process. We are pleased to see an approval role by the IPC for situations where minimal personal health information is required by the MOHLTC. The safeguards set out under sections 47 and 48 of the draft legislation add a rigour to the directed disclosure process by requiring thorough analysis of ways to minimize the impact on the privacy of the individual. This is a major improvement over Bill 159 and a most welcome addition.

Genetic Information (sections 2, 8(1)2, 19(2)(b), and 54, page 71)

Does the definition of "genetic information" accurately reflect the type of information that ought to be covered by these rules?

What, if any, protections should the Act contain to protect the privacy of an individual's genetic test information?

Legislative protection of genetic information has long been an objective of the IPC, and we are pleased to see the inclusion of the specific provisions in the draft legislation. As early as 1992, in our *Submission to the Ontario Law Reform Commission Project on Genetic Testing*, the IPC argued the need to regulate private sector intrusions into genetic privacy. More recently, in our 2000 *Annual Report*, we indicated our hope that provincial health privacy legislation would adequately regulate the collection, use and disclosure of genetic information.

Clause 2 of section 8(1) requires express consent by all organizations collecting, using and disclosing genetic information. In addition, section 19(2)(b) is an explicit requirement not to make the provision of genetic information a condition of dealing with an individual. These requirements are key to appropriate and effective protection of genetic information under the draft legislation.

The IPC's concern about the definition of genetic information is not about its scope, but rather its ability to be easily understood. Although the legislation will regulate the actions of doctors and genetic researchers, it also needs to be comprehensible to the lay person. The exact meaning of terms like "predictive information" and "routine physical measurements" is not obvious. We note that the definition of genetic information in the legislation of a number of American states (e.g., Connecticut H 6527, Hawaii S 1565, Maine 24-A 2159-C) is much simpler. For example:

> Genetic information: The information about genes, gene products or inherited characteristics that may derive from an individual or family member.
> (Connecticut H 6527)

The IPC encourages the government to revisit the definition to see if a plain language version is possible.

Data Matching (section 55, page 71)

MCBS wanted to include … section [55] in the consultation draft to facilitate a discussion on its content. In the final version of the legislation, a number of these subsections may be moved to regulation.

Section 6(2) excludes personal health information collected, used and disclosed by a health information custodian from FIPPA, and its municipal counterpart. Therefore, this information, in the custody and control of health information custodians, would not be covered by Management Board Secretariat's computer matching directive and guidelines. If the data matching provisions are removed entirely from the draft legislation, then there would be no legislative requirement to restrict data matches using personal health information. Therefore, the IPC supports including a requirement to undertake data matching assessments in the draft legislation, but agrees the provisions outlining the process could be moved to the regulations. The IPC's recommendations for amending the provisions, even if they are included in regulations, are outlined in Appendix C.

Procedures for Access (sections 56-61, page 74)

Do you find it confusing or unnecessary to have separate access rules in one Act?

Do you think the access rules should be distinct for health information custodians?

The access to information procedures are another example of how the draft legislation is difficult to read and understand, as one might expect by having two different regimes. These sections are at best repetitious, at worst confusing. Also, where there are differences between access to personal information and access to personal health information, no justification has been provided. The IPC is at a loss to understand why two different access regimes are required, and recommends streamlining the draft legislation by creating one combined process.

There may be a need to limit access to personal health information on the basis that it may result in serious harm to the treatment or recovery of an individual. However, this could be accommodated by a specific provision in a general access regime. It does not justify an entirely separate access process for personal health information in the custody of health information custodians.

There are a number of provisions in the proposed access process for personal health information not contained in the general access provisions. Analysis of these sections suggests no apparent reason for this difference, other than a failure to properly merge two separate regimes. For example:

- The health access scheme contains a statement that informal access procedures are not precluded (section 58(3)).
- The health access provisions go into greater detail than the general access provisions on some issues, e.g., abandoned requests (section 59(4)) and the meaning of "contact" (section 59(5)).

If these are necessary provisions, then they should be extended to all organizations. If not, they should be eliminated from the draft legislation.

Also, there is significant duplication between the two access schemes, adding needlessly to the length and complexity of the draft legislation. For example:

- the request for access must be in writing (sections 57(1) and 59(1));
- the organization/custodian has an obligation to provide assistance (sections 57(2) and 59(3));
- frivolous and vexatious requests (sections 57(6) and 60(6));
- obligation on organization/custodian to confirm identity of the individual (sections 57(10) and 60(9));
- duty to sever information that the individual is not entitled to (sections 57(11) and 60(10)); and
- response time and extension of the response time (sections 57(3), 57(4) and 60(3)).

The draft legislation would be shortened significantly if this duplication is eliminated.

The complicated nature of the parallel access schemes stands in contrast to the correction provision (section 62). There is a single process for an individual to request a correction to inaccurate personal information or records held by an organization, including health information custodians. Where there is a need for a provision addressing only custodians, that is done by way of a specific, limited subsection, rather than an entirely separate series of similar provisions. We commend this approach and strongly suggest that it be followed throughout this part of the draft legislation.

Do you think the roles envisioned for the Consent and Capacity Board and the Commissioner are appropriate in the process of accessing personal health information?

When a health information custodian believes granting access to an individual's personal health information reasonably may be expected to result in serious harm to the treatment or recovery of the individual or others, the custodian may refuse access. In the current draft, that decision may be appealed to the Consent and Capacity Board, but not to the IPC. What is the reason for this departure? The IPC does not support the inclusion of this process in the draft legislation. Neither does the OMA, as indicated at a meeting on September 17, 2001, involving the MOHLTC, the IPC and the OMA.

Under Alberta's *Health Information Act*, Manitoba's *Personal Health Information Act* and Saskatchewan's *Health Information Protection Act*, refusals to grant access to personal health information based on harm are appealed in the same manner as any other refusals to grant access. Similarly, under Bill 159, refusals to grant access based on harm could be appealed to the IPC. We are perplexed as to the change in the appeal process.

To the best of our knowledge, concern about the appeal to the IPC was not raised as an issue among health sector stakeholders during the public hearings on Bill 159. In the absence of such concern, it is not clear why the draft legislation provides a different type of appeal mechanism, involving the Consent and Capacity Board, for refusal to grant access based on harm. The distinct appeal process for refusals to grant access based on harm adds needless complexity to the legislation.

In addition, an appeal to the Consent and Capacity Board creates the potential for jurisdictional issues when a case may need to be adjudicated by both the IPC and the Board. This will result in unnecessary delays which are a disservice to all parties involved in the case. It may also create confusion as to who has oversight over what matters.

Under the public sector legislation, the IPC deals with a wide spectrum of issues on access appeals, including personal health information. We have the expertise necessary to make the types of decisions envisioned by section 61, as well as the ability to consult with, employ or retain experts

in any particular case. This could include consultation with health care professionals should a question arise as to whether granting access to a health record may be reasonably expected to result in serious harm to the treatment or recovery of the individual.

The IPC recommends removing the appeal to the Consent and Capacity Board from the draft legislation. Additionally, if the government thinks it necessary, the inclusion of a provision in the draft legislation could expressly recognize the Commissioner's ability to consult on such questions.

Fees (sections 32, 57 and 59, pages 40, 79 and 83)

An individual's right of access to his or her own personal information should not be limited by cost. Therefore, on principle, the IPC opposes the charging of fees under privacy legislation.

However, if fees are to be charged under this legislation, the IPC recommends making the criteria outlined under sections 57(12) and (13) applicable to all access requests for all types of personal information.

Finally, the IPC is confused by section 32. If it relates to prescribing a schedule of fees for access to personal health information in the custody and control of health information custodians, why is it not located with the other fee provisions in Part V? If the purpose of this section does not relate to fees for access, then the reason for including it in the privacy legislation is unclear.

Complaint Process (sections 63-69, page 89)

Is the complaint process clear? Do you have any suggestions for its improvement?

The complaint process is generally clear. The IPC's suggestions for improvement to the complaint process are set out below.

Mediation time frame

Sections 64(1)(b) and (c) give the IPC the authority to require a complainant to try to effect a settlement with the organization in question, or to authorize a mediator to try to effect a settlement, both within a time specified by the Commissioner. However, in many cases, it is not possible to determine up-front the complexity of issues, or estimate what a reasonable time period would be to try to resolve the issues through mediation. We recommend the draft legislation not require the Commissioner to specify a time period. Instead, the Commissioner should have the discretion to specify a time period, when it is appropriate to do so.

Mediation privilege

The IPC's preference is to have this provision mirror section 51 of FIPPA. Alternatively, section 64(2) should be narrowed. As currently worded, it is overly broad. While restricting the use and disclosure of mediation privileged information, it also may capture information that would not be considered subject to mediation privilege. To avoid this problem, the section should include a reference to "mediation privilege," a term defined by the common law.

Burden of proof where access denied

Section 64(11) states the burden of proving the refused individual is not entitled to access to a record of personal health information lies with the health information custodian that refused access. The burden of proof in cases of a denial of access to any personal information should always lie with the party who refused access, not just in the personal health information context. Therefore, section 64(11) should be expanded to cover all cases where access to personal information is refused by any type of organization under this legislation.

Warrants and the *Provincial Offences Act*

The reference to the *Provincial Offences Act* in sections 66(3) and 66(8) is inappropriate and should be removed. That legislation applies only to offences, and the IPC would not be engaging in investigations of offences under Part VI. The draft legislation should be amended to include a specific warrant provision similar to, for example, section 33(8) of the *Human Rights Code*.

Commissioner's Powers (Part VI, page 89)

Will the powers given to the Commissioner allow the legislation to be effectively enforced? Does the Commissioner's Office need further powers to fulfil its role? Do you think the Commissioner has been given too many powers?

Generally, the IPC supports the scope of the powers provided under sections 64 and 74. Our most serious concern relates to the fact that the Commissioner cannot require an individual to give testimony.

The investigation the IPC conducted into the disclosure of personal information by the Province of Ontario Savings Office (POSO) (report tabled with the Legislative Assembly in April 2000) provides ample evidence of the weaknesses of the current public sector oversight mandate, in particular the inability to compel testimony. In the POSO investigation, the IPC was unable to conduct a thorough investigation into the disclosure of sensitive financial data, primarily because a number of key individuals refused to be interviewed. The result was a report that could not satisfy the public's right to know the full details of a public institution's non-compliant use of personal information.

As this case demonstrates, without clear authority to compel testimony as part of the evidence gathering process, an oversight body cannot adequately assess the extent to which organizations are complying with their responsibilities. In turn, the public cannot be confident that organizations are being held accountable for their information management practices.

In virtually every other jurisdiction with similar legislation, including Canada (federal), Alberta, Saskatchewan, Manitoba, Quebec, Australia and New Zealand, the privacy oversight bodies have the power to require testimony. There is no reason why Ontario should fall short in this critical area. Also, without this power, the draft legislation may run a serious risk of not being considered substantially similar to the PIPEDA. What justification exists for this exclusion?

Another concern relates to the power to compel the production of records. We recommend the wording of section 66 be clarified to make it clear that the Commissioner's power to compel the production of records is not conditional on entering a premise during the course of an inspection. This would be similar to the powers specified under section 52(4) of FIPPA, section 12(1)(a) of PIPEDA, and section 88(2) of Alberta's *Health Information Act*.

Notice of Complaint to Affected Parties (section 64(7), page 91)

Should the Commissioner also be required to provide notice of the complaint to other parties that may be affected by the complaint?

The Commissioner should be required to notify the organization about whom the complaint is made (section 64(7)). However, notice to other affected parties should be left to the Commissioner's discretion. Depending on the circumstances, it may not be necessary or appropriate for the Commissioner to notify other parties (e.g., it would be more appropriate for the organization to notify the affected parties).

Appeal of IPC Orders (section 70, page 99)

Should any other parties be allowed to appeal an order, such as, other companies who may be affected by the order?

Are you satisfied with this appeal process or do you have any suggested improvements to it?

The IPC believes the right of appeal to the Divisional Court under section 70 is both unwarranted and unnecessary. Our experience suggests that it is in the best interests of the parties to a complaint, and of the public, to be able to rely on the Commissioner's decisions as final. In that case, there is no concern the process will be unduly extended, or made more complicated and expensive, by a court process. In our view, the right of appeal to the Divisional Court on an issue of law will be used disproportionately by organizations, to the detriment of the individual.

Therefore, the IPC strongly recommends that, as is the case under public sector legislation, the orders of the Commissioner should be final and binding, without a right of appeal. The IPC's orders would continue to be subject to judicial review, to permit those cases that raise serious jurisdictional issues to proceed to court. This would be consistent with similar legislation in other jurisdictions such as Alberta, Australia and New Zealand, where no right of appeal exists.

Alternatively, if the right to appeal is not removed, the appeal should proceed only where the Divisional Court grants leave to appeal. This would help ensure that only matters that truly warrant the court's consideration are subject to appeal. In addition, the right of appeal should be narrowed to exclude matters relating to access and correction. This would ensure that an appeal may not be used to unnecessarily delay an individual's access to, or correction of, his or her own personal information.

Enforcement of IPC Orders (section 71, page 101)

Do you agree with this approach to enforcing the Commissioner's orders?

The IPC is satisfied with the approach outlined in the draft legislation for enforcing the Commissioner's orders (section 71).

Damages (section 73, page 102)

In your opinion, are the factors listed below appropriate for a court to consider when making an award for damages?

Is this approach adequate to compensate people who have suffered losses due to violations of this Act?

The IPC has no objections to the factors listed in section 73 for a court to consider when making an award for damages, or concerns with the approach to compensation. The approach outlined in the draft legislation is adequate.

Assistant Commissioners (section 75, page 103)

Section 4(4) of FIPPA enables the Commissioner to appoint Assistant Commissioners in a manner that he or she thinks appropriate. By specifying the number and type of Assistant Commissioners in section 75 of the draft legislation, and again in the consequential amendments to FIPPA, the government is constraining the independence of the Commissioner and the flexibility of that office. We would prefer the draft legislation give the IPC the discretion to appoint Assistant Commissioners as warranted. We accept, however, the need for a dedicated Assistant Commissioner for Health.

Offences (section 79, page 106)

Are there other offences that should be included in the list?

Should some proposed offences be removed from the list?

Are the penalties for being found guilty of an offence adequate?

As the IPC noted in our September 2000 submission on the *Consultation Paper: Proposed Ontario Privacy Act*, we believe that while the legislation should provide for offences in limited cases involving wilful misconduct, the primary focus of the enforcement provisions in privacy legislation should be on educating organizations not complying with the legislation, and ensuring they take appropriate steps to reduce the risk of any future privacy breaches.

The IPC recommends amending section 79(1)(b) so correction is covered in a manner consistent with section 61(1)(c) of FIPPA.

In addition to an offence under section 79(1)(h), there needs to be a provision relating to redress for the whistleblower. The draft legislation should be amended to add remedies, such as reinstatement and compensation, for the individual. This may be done through the court on conviction of the offence, or through an application by the whistleblower to the Labour Relations Board, as in the case of the *Environmental Bill of Rights* (Part VII, ss. 104 to 116).

The penalties stipulated in section 79(4) seem adequate.

Regulations (section 80, page 108)

At several points in the consultation draft, the government noted that provisions may be moved out of the body of the legislation into the regulations. The IPC believes it is in the public's interest to have substantive matters addressed within the actual legislation. However, in this submission we have agreed it might be appropriate to move certain provisions with limited application to regulations. The inclusion of these provisions in regulation will not result in an erosion of the fundamental rights and responsibilities set out in the draft legislation.

Overall, the regulation provisions in the draft legislation are too broad. Below are specific examples of sections that should be removed because they significantly compromise individuals' rights and organizations' responsibilities.

Section 80(1)(g) enables specific organizations or classes of organizations, including health information custodians, to be pulled outside of the scope of the legislation without any public consultation or accountability. This completely subverts the purpose of the legislation. There is enough scope in the other regulation provisions to accommodate the special needs of all manner of organizations, while at the same time, maintaining the privacy rights of the individual.

Section 80(1)(n) permits the government, without public consultation or accountability, to exempt organizations from acting in conformity with their information practices. There may be a need to prescribe certain requirements for information practices, as specified under section 80(1)(m), but we believe an exemption from these practices is unacceptable.

In terms of the rights of the individual, section 80(1)(j) is completely inappropriate as it permits the government, without public consultation or accountability, to restrict the rights of the individual. The draft legislation recognizes the ability to withdraw consent as an essential component of informed consent. Section 12 already contains five reasonable limitations on the right to withdraw consent. Any additional reasons should be specified in the legislation.

As noted in our discussion of ambiguities under the draft legislation, we are concerned about sections 80(4) and (5). If these sections are intended to permit the development of sectoral or industry codes of practices that may increase or decrease the privacy standards, akin to Codes of Practice under New Zealand's *Privacy Act, 1993, (as amended)* (sections 46-52, Part VI), a number of additional requirements are essential. In particular, the scope, content, method of public consultation, and the Commissioner's role need to be defined in the legislation. The IPC is also concerned that the use of codes may bring into question the draft legislation's potential for substantial similarity to PIPEDA. Regardless of the scope of the codes, the draft legislation should make it clear that they should not be permitted to diminish an individual's right of access and correction.

In our comments on Bill 159, the IPC made it clear there is a need for transparency and public accountability when creating exceptions to privacy protections in the legislation. Broad regulation-making powers constitute a potential back door for avoiding the protections of personal information, and the duties and responsibilities set out in the legislation. This lack of transparency is not addressed in the draft legislation, and it is even more troubling to the IPC given the broad scope of the legislation.

To address our concerns, we recommend the addition of provisions making the entire regulation-making process more open. Transparency in the regulation-making process is integrated into Ontario's *Environmental Bill of Rights* (Part II, Public Participation in Government Decision-Making), and Quebec's *Regulation Act* (Division 1, Interpretation and Application). The IPC's suggestions for how to achieve more openness and accountability in the regulation-making process are outlined in Appendix D.

Drafting Issues

The IPC has a number of questions related to the drafting of the regulation provisions:

- Why is section 80(1)(a) necessary? It seems to be saying that a regulation may be prescribed on any provision in the Act that says regulation may be prescribed.
- What is an example of what is being contemplated by section 80(1)(h)?
- Should there be references in sections to alert the reader to the existence of a relevant regulation? For example, should there be something in section 37(3) indicating that conditions may be prescribed in a regulation under section 80(1)(k)? Similarly, should there be a reference to a possible regulation under section 80(1)(m) in section 53(1)?

Quality of Care Information Protection Act (page 115)

Are the provisions in this Act appropriate and effective for achieving this quality of care mandate? Do you have any suggestions for improving upon this proposed bill?

The IPC does not have any specific concerns about the provisions for achieving the quality of care mandate, but we are concerned about the absence of any oversight for these provisions.

Under section 58(1)(a), quality of care information is excluded from the individual's right of access. In addition, under section 63(1), an individual in not entitled to complain to the IPC about what constitutes quality of care information. We do not support these exclusions, and note that all other exceptions to the right of access are subject to independent review by the IPC. The individual should be able to ask the Commissioner to review the information the custodian has deemed to be quality of care information, in order to determine the correctness of that designation.

It is possible that organizations might apply an overly broad interpretation of what is quality of care information and, consequently, put unreasonable limits on the individual's right of access to personal health information. Under the draft legislation, there is no mechanism to rectify this situation. Therefore, the draft legislation should be amended to enable the individual to complain to the IPC about what constitutes quality of care information. This would ensure the necessary oversight for all exceptions to the individual's general right of access to personal health information.

Title

Finally, a brief comment about the title of the *Privacy of Personal Information Act, 2002*. Privacy is a value that is always relative to an individual, not to a type of information. Information does not have privacy, but its protection is essential to an individual's privacy. The draft legislation is a data protection statute and, therefore, the title should reflect that purpose. The IPC recommends changing the title to "Personal Information Protection Act" or to "Privacy Protection of Personal Information Act." This change to the title would make it more accurate, and it also would make it more consistent with current legislation such as the *Freedom of Information and* ***Protection of Privacy*** *Act* or the federal ***Personal Information Protection*** *and Electronic Documents Act* [emphasis added].

Appendix A – Inconsistencies

Privacy of Personal Information Act, 2002	IPC Suggested Changes
PART I **INTERPRETATION AND APPLICATION**	
Definitions	
2. In this Act, … "de-identify", in relation to the personal information of an individual, means to remove any information that, … (c) can be linked or matched by a reasonably foreseeable method to other information that identifies the individual or that can be used or manipulated by a reasonably foreseeable method to identify the individual,	**2.** In this Act, … "de-identify", in relation to the personal information of an individual, means to remove any information that, … (c) can be linked or matched by a reasonably foreseeable method to other information that identifies the individual or that can be ~~used or~~ manipulated by a reasonably foreseeable method to identify the individual, **Comment** Change needed for consistency with definitions of personal information and personal health information.
"organization" includes a person, an association whether or not incorporated, a partnership, a health information custodian, a trade union and an individual, other than an individual acting in a personal and non-commercial capacity;	"organization" includes a person, an association whether or not incorporated, a partnership, a health information custodian, a trade union and an individual, other than an individual acting in a personal ~~and~~ non-commercial capacity; **Comment** The wording of the definition under section 2 is not consistent with section 7(1)(a). Need to amend one or the other of the sections.

Privacy of Personal Information Act, 2002	**IPC Suggested Changes**
PART III **COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION**	
Disclosures related to this or other Acts	
44. Subject to section 41, a health information custodian may disclose personal health information about an individual without the consent of the individual, … (g) to a person carrying out an inspection, investigation or similar procedure that is authorized by a warrant or **under an Act of Ontario, Canada or a province or territory of Canada other than Ontario**; (h) if authorized or required by or **under any other Act or an Act of Canada or a province or territory of Canada other than Ontario** or a treaty, agreement or arrangement made under any of those Acts; or (i) for the purpose of having a legally authorized person or body carry out legally authorized activities to administer or enforce **any law of Canada or a province or territory of Canada** or a by-law of a municipality. [emphasis added]	**Comment** There is a need to make the wording of commonly referenced items, such as other laws, consistent. As currently worded, the reader is left trying to figure out if the differences mean anything – are they deliberate or inadvertent? Inconsistency in language needlessly confuses the provisions.

Appendix B – Enhancing Privacy Protections

Privacy of Personal Information Act, 2002	IPC Suggested Changes
PART III **COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION**	
GENERAL LIMITATIONS	
Disclosure outside Ontario	
28. (1) An organization shall not disclose personal information collected in Ontario to an organization outside Ontario unless, …	**28.** (1) An organization shall not disclose personal information collected in Ontario to an organization outside Ontario unless, …
(b) the disclosing organization believes on reasonable grounds that the organization receiving the information will take appropriate steps to preserve the confidentiality of the information.	(b) the disclosing organization believes on reasonable grounds that the organization receiving the information will take appropriate steps to preserve the confidentiality of the information **and to protect the privacy of individuals; and**
	(c) the organization receiving the information is statutorily or contractually bound to maintain the confidentiality of the information and to protect the privacy of individuals, not to use the information for any purpose other than that for which it is being disclosed, and not to disclose it to any other party.
	Comment These additional safeguards would be consistent with the suggested requirements for disclosure to an organization or its professional advisors within Ontario, as specified in section 37(1)(j).

Privacy of Personal Information Act, 2002	**IPC Suggested Changes**
Marketing	
31. (1) An organization shall not use or disclose personal information about an individual to market goods or services or for market research unless the individual consents. **No disclosure for consideration** (2) A health information custodian shall not disclose, for consideration, personal health information about an individual under subsection (1), even if the individual consents.	**31.** (1) An organization shall not use or disclose personal information about an individual to market goods or services or for market research unless the individual consents. **No disclosure ~~for consideration~~** (2) A health information custodian shall not disclose~~, for consideration,~~ personal health information about an individual under subsection (1), even if the individual consents. **Comment** Personal health information should not be disclosed for marketing purposes, regardless of whether there is any consideration.

Privacy of Personal Information Act, 2002	**IPC Suggested Changes**
PART IV **DUTIES OF ORGANIZATIONS WITH RESPECT TO ~~RECORDS OF~~ PERSONAL INFORMATION**	
GENERAL	
Notes of uses and disclosures without consent	
51. (1) An organization shall make a note of all uses and disclosures that it makes of personal information about an individual without the individual's consent except if the individual would not be entitled to access to the information under subsection 56 (1) or a record of the information under subsection 58 (1).	**51.** (1) An organization shall make a note of all uses and disclosures that it makes of personal information about an individual without the individual's consent ~~**except if the individual would not be entitled to access to the information under subsection 56 (1) or a record of the information under subsection 58 (1).**~~ **Comment** The organization should be required to make a note of all uses and disclosure of personal information without the individual's consent. In most cases, the organization would have no way of definitively determining at the time of the use or disclosure whether the individual would be entitled to access the information under section 56(1) or a record of the information under section 58(1). A decision to refuse access under sections 56(1) or 58(1) could be appealed and not upheld by the Commissioner. Also, if notes are made the organization will know who to notify in the event that the personal information is corrected.

Privacy of Personal Information Act, 2002	**IPC Suggested Changes**
Duty to follow practices	
53. (2) The organization shall act in conformity with its information practices except if the regulations specifically permit the organization not to do so.	~~**53.** (2) The organization shall act in conformity with its information practices except if the regulations specifically permit the organization not to do so.~~ **Comment** Exceptions should not be specified in regulations.
Information for public	
53. (4) The organization shall, in a manner that is practical in the circumstances, make available to the public a written statement that, … (d) describes how to make a complaint to the Commissioner under this Act.	**53.** (4) The organization shall, in a manner that is practical in the circumstances, make available to the public a written statement that, … (d) describes how to make a complaint **to the organization and** to the Commissioner under this Act. **Comment** The Challenge Compliance principle of PIPEDA (4.10.3) requires an organization to inform the individual of its own complaint process. We recommend making this obligation explicit in the draft legislation. This is particularly important given sections 53(3)(d) and 64(5)(b) which suggest that an organization will have the opportunity to address a complaint before it is reviewed by the Commissioner.

Appendix C – Data Matching

Privacy of Personal Information Act, 2002	IPC Suggested Changes
PART IV **DUTIES OF ORGANIZATIONS WITH RESPECT TO RECORDS OF PERSONAL INFORMATION**	
PERSONAL HEALTH INFORMATION	
Exceptions (Data Matching)	
55. (2) This section does not apply to a data matching if, …	**55.** (2) This section does not apply to a data matching if, …
(c) the purpose of the matching is to evaluate the utilization or effectiveness of an existing program or service;	~~(c) the purpose of the matching is to evaluate the utilization or effectiveness of an existing program or service;~~
(d) the purpose of the matching is to ensure that personal information is accurate and current and to update the information;	~~(d) the purpose of the matching is to ensure that personal information is accurate and current and to update the information;~~
(e) the purpose of the matching is to reconcile financial information; or	~~(c) the purpose of the matching is to reconcile financial information; or~~
(f) the purpose of the matching is one that is prescribed.	~~(f) the purpose of the matching is one that is prescribed.~~ **Comment** To protect the privacy of individuals, the exceptions to the computer matching requirements should be as narrow and specific as possible. The criteria set out under section 55(1) should determine whether or not the section applies. The proposed exceptions (c) through (f) to the data matching requirements are not appropriate if the results of the matching could potentially directly affect an identifiable individual or a class of identifiable individuals.

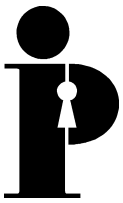
Privacy of Personal Information Act, 2002	**IPC Suggested Changes**
Contents of assessment	
55. (5) A privacy impact assessment shall include the matters that are prescribed.	**55.** (5) A privacy impact assessment shall ~~include the matters that are prescribed.~~, **(a) name the participants in the computer matching or describe the class to which they belong in a manner that is sufficient to identify them;** **(b) describe the type and number of records to be compared by the computer matching;** **(c) describe the type of records that will result from the computer matching;** **(d) set out the purpose or purposes, as the case may be, for which the records resulting from the computer matching will be used or disclosed;** **(e) set out the authority under this Act for each collection, use and disclosure of records of personal health information that the computer matching will involve;** **(f) state the duration of the computer matching;** **(g) set out the administrative, technical and physical safeguards and practices that the participants in the computer matching will implement in relation to the matching to ensure the security, accuracy and integrity of the records of personal health information involved in the matching;** **(h) set out an analysis of the expected costs and benefits of the computer matching;**

Privacy of Personal Information Act, 2002	IPC Suggested Changes
Contents of assessment (cont'd)	
	(i) describe when and how individuals who may be directly affected by the computer matching have been or will be notified about the matching or explain why individuals who may be directly affected by the matching will not be notified; and **(j) specify the procedures that will be used for verifying any information the computer matching produces.** **Comment** The content of the privacy impact assessment should be set out in the legislation. Alternatively, indicate in this section that the IPC will prescribe the contents.
Verification of information	
	55. (5.1) Before using any information resulting from the computer match, the health information custodian must, **(a) notify the affected individuals; and** **(b) verify that the information produced by the computer match is correct.**
Information for the public	
	55. (7.1) All privacy impact assessments and comments, if any, offered by the Commissioner should be made available by the health information custodian to the public, upon request.
Same	
	55. (7.2) Every health information custodian shall provide to the public, upon request, a description of the computer matching activities it has participated in the during the previous year.

Appendix D – Transparency in Regulation-Making

Privacy of Personal Information Act, 2002	IPC Suggested Changes
PART VII MISCELLANEOUS	
Public Notice	
	80. (6) The minister shall give notice of a proposed regulation in the Ontario Gazette, on the Ministry's Web site, and by any other means the minister considers appropriate. This notice shall be given at least 45 days before the deadline for submitting comments on the proposed regulation unless the minister determines that a shorter time is required. Contents of notice of proposed regulations: Notice of a proposed regulation shall include the following: 1. A brief description of the proposed regulation as well as the full text of the proposed regulation. 2. A statement of the manner by which and the time within which members of the public may participate in decision-making on the proposed regulation. 3. A statement of where and when members of the public may review written information about the proposed regulation. 4. An address to which members of the public may direct i. written comments on the proposed regulation; and ii. written questions about the rights of members of the public to participate in decision-making on the proposed regulation.

Privacy of Personal Information Act, 2002	IPC Suggested Changes
Public Notice (cont'd)	
	5. Any information prescribed by the regulations under this Act. 6. Any other information that the minister considers appropriate. Rights of participation A statement shall include a description of the right to submit written comments in the manner and within the time specified in the notice. Exception: Emergencies (1) The time for submitting comments may be shortened or the regulation may be made without publishing a notice and providing an opportunity for comments if the urgency of the situation requires it. (2) If the minister decides under subsection (1) not to give notice of a proposed regulation, the minister shall give notice of the decision to the public and to the Information and Privacy Commissioner. (3) Notice under subsection (2) shall be given as soon as reasonably possible after the decision is made and shall include a brief statement of the minister's reasons for the decision and any other information about the decision that the minister considers appropriate. (4) Every regulation, and every amendment or revocation of a regulation, issued in accordance with this section shall be identified as a temporary regulation or amendment or revocation, and shall remain in force for such period (not exceeding one year after the date of its issue) as is specified for that purpose in the regulation or, as the case may be, the amendment or the revocation.



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca