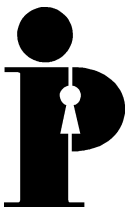
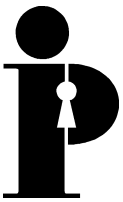
Information
and Privacy
Commissioner/
Ontario

Submission to the Ministry of Health and Long-Term Care in Response to *Ontario's Proposed Personal Health Information Privacy Legislation for the Health Sector (Health Sector Privacy Rules)*



Ann Cavoukian, Ph.D.
Commissioner
October 2000



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.

Introduction

The Office of the Information and Privacy Commissioner of Ontario (IPC) has a mandate under the *Freedom of Information and Protection of Privacy Act* to review and comment on the privacy protection implications of proposed legislative schemes. The proposed personal health information privacy legislation for the health sector will have a significant impact on the privacy of every individual in the province of Ontario. The establishment of a comprehensive framework to protect personal health information has been anticipated by members of the public, health care providers, and other stakeholder groups since the publication of the *Report of the Royal Commission on Confidentiality of Health Information in Ontario* (the Krever Commission Report) in 1980.

The IPC has always supported the implementation of legislated privacy protection rules for health information in Ontario. We participated in both rounds of consultations on the proposed health information privacy legislation, and made a number of formal and informal submissions on successive drafts of the previously proposed *Personal Health Information Protection Act*. After more than fours years of work, the Ministry of Health and Long-Term Care is now in the final stages of preparing the proposed health sector privacy rules.

We recognize the considerable effort that has been invested in developing privacy rules for the health sector. However, in light of other recent initiatives to regulate privacy in the private sector, we have some concerns about the plan to proceed with the implementation of this initiative now. Since the consultations on privacy legislation for Ontario's health sector began in 1996, the federal *Personal Information Protection and Electronic Documents Act* (formerly Bill C-6) has been passed. In addition, the province of Ontario has embarked upon consultations on broad, private sector privacy legislation.

At this point in time, it is not clear how the proposed privacy rules for the health sector will compare to those that will eventually be introduced for other sectors in the province. There is also considerable ambiguity about how the two pieces of substantially different provincial legislation will work together, and in conjunction with the federal legislation. Consequently, our preference is for the Government of Ontario to proceed with the implementation of broad private sector privacy legislation now, and to have the health sector privacy rules developed within the context of the broader legislative framework.

In this submission, we make specific comments and suggestions to enhance the privacy protection framework being proposed for the health sector. Rather than limit our comments to responding to just the five sets of questions, we have organized our comments in accordance with the major headings from the consultation paper, *Ontario's Proposed Personal Health Information Privacy Legislation for the Health Sector (Health Sector Privacy Rules)*, prepared by the Ministry of Health and Long-Term Care. Reference to the consultation paper's page numbers are included in the headings of this submission.

Why Are Legislated Personal Health Information Privacy Rules Necessary? (MOH page 2)

In general, we agree with the identified goals of implementing legislated privacy rules for the health sector. These goals recognize the unique character of personal health information – as one of the most sensitive types of personal information that is frequently used and disclosed for a broad range of purposes that go beyond the provision of health care to the individual.

Nevertheless, to the greatest extent possible, we believe individuals should be given the right to control the collection, use, and disclosure of their own personal health information. We believe there is a greater societal, as well as individual, interest in protecting the privacy of personal health information. This interest should not be sacrificed unless there is clear justification and appropriate safeguards in place to minimize the impact on privacy.

How would the legislated health sector privacy rules relate to the proposed *Ontario Privacy Act*? (MOH page 4)

The Ontario Government recently concluded the consultation for its *Consultation Proposal for an Ontario Privacy Act*.[1] As indicated in our submission to the Ministry of Consumer and Commercial Relations, we commended the Government of Ontario for recognizing the need to proceed with provincial private sector privacy legislation. We also generally supported the four goals of Ontario's proposed private sector privacy legislation:

1. Comprehensive and seamless privacy protection
2. Flexibility for unique privacy needs and circumstances
3. Efficient, fair and effective enforcement
4. Compatibility with other laws.

In the Ministry of Health and Long-Term Care's consultation paper, the proposed privacy rules for the health sector are presented as being key to meeting the second goal – flexibility for unique privacy needs and circumstances. Although we do not disagree with the suggestion that the proposed health sector privacy rules will enhance flexibility, we believe that the public may be confused as to how these two initiatives fit together – one for private sector privacy legislation and the other for health sector privacy legislation in **both** the public and private sectors.

[1] A copy of the Ontario Government's *Consultation Paper: Proposed Ontario Privacy Act* may be found on the Ministry of Consumer and Commercial Relations' Web site: <www.ccr.gov.on.ca>.

A copy of the IPC's *Submission to the Ministry of Consumer and Commercial Relations in Response to A Consultation Paper: Proposed Ontario Privacy Act* may be found on the IPC Web site: <www.ipc.on.ca>.

Adding to the confusion is the fact that, unlike the proposed private sector privacy legislation, the proposed privacy rules for the health sector are not clearly based on the *Canadian Standards Association Model Code for the Protection of Personal Information* (CSA Model Code). This makes it difficult to compare the protections that will be provided by the health rules with those that will be provided under the private sector privacy legislation. The lack of conformity with the CSA Model Code also makes it difficult to see how the health sector privacy rules will harmonize with the proposed provincial private sector legislation and with the federal *Personal Information Protection and Electronic Documents Act*.

It is our view that the privacy provisions set out in the private sector privacy legislation should be sufficiently flexible to accommodate privacy needs in a range of contexts. Fair information practices, such as those set out in the CSA Model Code and embodied in the federal *Personal Information Protection and Electronic Documents Act*, are internationally accepted rules for the collection, use, and disclosure of personal information. They have been successfully applied to personal information in a broad range of contexts. In general, it is our view that basic privacy protection does not need to change from one situation to the next. Unique privacy needs arising in various contexts can be accommodated through narrowly defined and carefully worded exceptions that may apply under specific circumstances.

As noted in our submission to the Ministry of Consumer and Commercial Relations, we are not opposed to the inclusion of sector-specific codes in the broader private sector privacy legislation as one mechanism for enhancing flexibility. However, if there are sector-specific privacy rules, such as the proposed health privacy rules, there should be a clear rationale and the rules should be set out in a manner that is consistent with the broader legislative framework.

Accordingly, we suggest that, prior to introducing separate rules for the health sector, the implications and rationale for having separate rules and a different approach to privacy protection for the health sector need to be carefully considered. The Government should also consider how the various pieces of legislation will work together in light of the fact that the proposed health sector privacy rules generally do not conform to the standard CSA Model Code.

We do not oppose the incorporation of the proposed privacy rules for the health sector as a schedule to the *Ontario Privacy Act*, as indicated in the consultation paper, providing it is a schedule in the legislation, rather than under the regulations. This would ensure greater public debate and scrutiny for any future amendments. We believe such openness and accountability is necessary given the sensitive nature of personal health information.

How Has The Proposal For Legislated Health Sector Privacy Rules Been Developed? (MOH page 6)

The scope of the proposed legislation

We do not object to the narrowing of the scope of the legislation to focus more closely on the health sector because all organizations within the province will be subject to either public or the proposed private sector privacy legislation.

However, one issue that we believe needs to be clarified is the potential application of the proposed legislation to both private and public sector organizations in the health sector. This raises two concerns:

- First, public sector institutions that are custodians of personal health information, are already subject to Ontario's *Freedom of Information and Protection of Privacy Act* or the *Municipal Freedom of Information and Protection of Privacy Act*. When the health sector privacy rules are implemented, these organizations will be subject to two separate pieces of legislation. This could create considerable confusion.
- Second, if the health sector privacy rules are included as a schedule or a sectoral code under the broader private sector privacy legislation, the inclusion of public sector organizations in legislation created for the private sector could also create confusion.

Requirements relating to research (MOH page 7)

We support the proposal to strengthen the protections for personal health information used and disclosed for research purposes. The IPC recommended the inclusion of such safeguards in submissions on the previously proposed *Personal Health Information Protection Act*. Consistent with what was suggested in the consultation paper, it is our view that all research proposals involving the use or disclosure of personal health information should be subject to review by a research ethics review body. In addition, we agree the consent of the individual generally should be required, except in limited circumstances.

In approving a research proposal, one of the roles of the research ethics review body should be to balance the interests of the individual and the public good. Accordingly, we would like Ontario's privacy rules for the health sector to contain requirements similar to those for the review of research proposals under Alberta's *Health Information Act*. Specifically, the research ethics review body should be required to assess whether the research proposal could be carried out without personally identifiable health information. Where the research ethics review body determines that the research proposal cannot be carried out without personal health information, it should assess whether:

- the researcher should be required to obtain individual consent for the disclosure of personal health information to be used in the research;
- the proposed research is of sufficient importance that public interest in that research clearly outweighs the interest in protecting the privacy of the individuals involved;
- obtaining consent would be impractical or would compromise research results;
- the researcher is qualified to carry out the research;
- adequate safeguards will be in place to protect the privacy of individuals; and
- any specific conditions should be placed on the researcher.

In assessing whether the researcher should be required to obtain consent, the research ethics review body should consider the purposes for which the personal health information will be used by the researcher. In our view, it may not be necessary to require a researcher to obtain consent, providing that the following safeguards are put in place:

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

Where the researcher is proposing to contact individuals directly to obtain additional information, to invite participation in a primary research project, or for any other purpose, the consent of the individual to be contacted by the researcher for that purpose must be obtained beforehand. Alberta's *Health Information Act* and Manitoba's *Personal Health Information Act* both require consent before researchers can contact individuals.

In addition, Alberta's legislation contains specific criteria for a research ethics review body to use to assess whether the public interest in the proposed research outweighs the interest in protecting the privacy of individuals. Specifically, the research ethics review body must consider the extent to which the research contributes to the following:

- identification, prevention, or treatment of illness or disease;
- scientific understanding relating to health;
- promotion and protection of the health of individuals and communities;

- improved delivery of health services; or
- improvements in health system management.

The researcher only should be able to request access to personal health information from the custodian where the research ethics review body is satisfied that all of the requirements of the legislation will be addressed. Furthermore, if the custodian decides to disclose the personal health information to the researcher, based on the assessment of the research ethics review body, the researcher should be required to enter into an agreement with the custodian in which the researcher agrees to:

- comply with the proposed legislation and the regulations;
- comply with any conditions set out by the research ethics review body;
- not publish the health information in a form that could be used to identify an individual;
- not contact individuals, except where individuals have consented to being contacted by the researcher;
- use the personal health information only for the purpose set out in the research agreement;
- take reasonable steps to ensure the security and confidentiality of the information;
- dispose of the personal health information in the manner set out in the agreement; and
- allow the custodian to access or inspect the researcher's premises to confirm that the researcher is complying with all of the requirements set out in the agreement.

These requirements for research agreements have been drawn from health information legislation from other jurisdictions in Canada.

Requirement to record unanticipated disclosures (MOH page 8)

We support the proposal to require custodians to document all unanticipated uses and disclosures of personal health information made without the consent of the individual. We also agree that individuals should have a right to see this documentation under the same rules that would permit individuals to access their own personal health information. However, we want to stress that custodians should be required to make every effort to identify all reasonable uses and disclosures, and to make those known to the individual at the time of collection of the personal health information.

We endorse the proposal to require custodians to be open about their information management practices, and to make written information available to individuals about anticipated uses and disclosures of personal health information. This requirement for openness is an essential component of privacy protection, as it allows individuals to effectively exercise their rights under the legislation. We are pleased to see this as a component of the proposed privacy protection framework for the health sector.

To enhance openness, it is our view that, at the time when personal health information is collected, custodians should be required to inform individuals about all anticipated uses and disclosures (i.e., the purposes for which personal health information will be collected). We discuss specific openness requirements under the rules covering collection of personal health information.

It should be noted that regardless of whether a use or disclosure is anticipated or not, there are many ways to enhance openness that would not pose an undue burden on the organization. For example, custodians could fulfil the obligation for openness by posting signs in offices; by mailing bulletins to customers, clients, or patients on a periodic basis; or by providing brochures to individuals when they first contact the organization.

Use and disclosure of registration information (MOH page 9)

We like the addition of the proposed new principle that would prohibit the use and disclosure of personal health information in circumstances where the purpose could be met by registration information alone. Registration information is defined in the consultation paper as name, home address, date of birth, and marital status.

As suggested in the consultation paper, one example might be where personal information is used for health facility fundraising. Other examples of where it might be appropriate to permit the disclosure of registration information alone are contained in health information legislation from other jurisdictions.

For example, under Saskatchewan's *Health Information Protection Act*, registration information alone is permitted to be disclosed for purposes such as:

- verifying the eligibility of individuals to participate in a program or receive a service;
- verifying the accuracy of registration information; and
- planning, delivering, evaluating or monitoring a program.

In contrast, under Ontario's proposed health sector privacy rules, the disclosure of personal information for these purposes is not limited to just registration information. If registration information alone is sufficient for these purposes in Saskatchewan, it is not clear to us why the disclosure of more personal health information would be permitted for these purposes in Ontario. In our view, there should be a general prohibition against the use and disclosure of personal health information if registration information alone would be sufficient for the purpose of the use or disclosure. In addition, we believe that what constitutes registration information must be narrowly defined (e.g., is marital status appropriate or necessary?).

Patient's right to block disclosure for health care purposes (MOH page 9)

We have concerns with the proposal not to include a provision that would permit individuals to control the disclosure of personal health information to their health care providers. Instead, under the proposed health sector privacy rules, health care providers would have the discretion to disclose whatever personal health information they deem to be appropriate under the circumstances.

The so-called "lock box" provision, which would allow individuals to control the disclosure of their personal health information for health care purposes, is a key component of privacy protection. We recognize that the inclusion of the lock-box provision could, in some cases, allow individuals to withhold key personal health information that may be critical to their care and treatment. However, if there were no ability to control what information is disclosed to a health care provider, in some cases, extremely sensitive, subjective, personally damaging, irrelevant, or outdated personal health information could be disclosed.

The proposal to allow health care providers to determine what personal health information to disclose, in every instance, assumes that health care providers always know what should be disclosed in the best interest of individuals. However, the public may not agree with this assumption. *The Equifax Canada Report on Consumers and Privacy in the Information Age* (1994) indicated that close to one in five Canadians (18%) reported experiencing improper disclosures of their personal medical information. Respondents to the survey most frequently (8%) stated that a doctor who had treated them or their families had disclosed medical information about them in an improper way.

It is our view that the health care provider may not, in all cases, be in the best position to determine what is in the best interest of the individual. As individuals are provided with increasingly greater access to a broad range of health information through resources such as the Internet, they can and will play an increasingly greater role in their own health and well-being. Accordingly, it should not be assumed that the health care provider is in a better position than the individual to know what should be disclosed.

In an electronic world, the ability to control what information is disclosed to health care providers is essential for privacy protection. New information and telecommunications technology allows for the creation of an electronic patient record containing a cradle-to-grave medical history of the individual that can be readily shared among a variety of health care providers, and beyond, with the push of a button. Since the electronic patient record will be accumulated over a much longer period of time than most paper-based medical records, the likelihood that it will contain outdated and perhaps irrelevant information is increased. Also, in comparison to most paper-based medical records, the cradle-to-grave electronic patient record is more likely to contain sensitive information that the person does not want widely shared. For example, it might contain information about abortions, sexually transmitted diseases, sexual orientation, substance abuse, psychological problems, etc. While this type of information might be critical in some health care situations, in other circumstances, it may not be relevant.

If individuals have no control over the personal health information contained in their electronic patient record or how that information is disclosed, they may engage in activities to prevent information from being added to their record. For example, individuals could withhold certain sensitive information or provide inaccurate information out of fear that the information will make its way onto their electronic patient record that could be made indiscriminately available to all of their health care providers and, perhaps, other secondary users of personal health information. In addition, individuals who have concerns about the use and disclosure of their health information may avoid seeking treatment altogether. If the electronic patient record contained inaccurate or incomplete information, its usefulness for providing health care to the individual and for secondary purposes (e.g., planning and medical research) would be diminished.

There is some evidence to suggest that people may withdraw from full participation in their own health care if they are afraid their personal health records will fall into the wrong hands and lead to discrimination, loss of benefits, stigma, and unwanted exposure. A 1999 survey by the California HealthCare Foundation found that one in six people engages in what they refer to as "privacy protective behaviour" to shield themselves from the misuse of their personal health information. This privacy protective behaviour may include lying to doctors, providing inaccurate information, doctor-hopping, and avoiding medical care altogether. To the extent that individuals are able to control what information is disclosed to health care providers, it is more likely that this type of behaviour would be minimized.

We strongly believe that individuals should have the right to control their personal health information, particularly in terms of secondary uses and disclosures. This must be the essential core of the proposed privacy rules for the health sector. If not the lock box, then the rules for non-consensual disclosure must be significantly narrowed. "Professional judgment" is not sufficient to override individuals' express wishes not to have some of their personal health information disclosed. At a minimum, the legislation should define when such disclosures would be appropriate.

We also believe individuals should be able to prohibit disclosure of personal health information via electronic means. Such a right would be consistent with the rights of individuals provided under health information protection legislation from other jurisdictions in Canada. For example, under Alberta's *Health Information Act*, a custodian cannot disclose personal health information via electronic means without the individual's consent, except for billing purposes. Under Saskatchewan's *Health Information Protection Act*, individuals have the right to require a custodian not to store a record or part of a record of their personal health information on the networked electronic health record maintained by the Saskatchewan Health Information Network or on any other prescribed network. Where personal health information is stored on the networked electronic health record, individuals may require a custodian to prevent access by other organizations to all or part of the information on the network.

Computer matching **(MOH page 10)**

We agree that the privacy rules for the health sector should include provisions for computer matching. This is particularly important in light of the intent to apply the rules to public bodies. Public bodies are already required to comply with a computer matching directive that provides a number of privacy safeguards. These safeguards include the completion of a computer matching assessment that must be submitted to the IPC for review and comment.

We support the proposal to require custodians subject to the *Freedom of Information and Protection of Privacy Act*, or the municipal equivalent, to prepare and submit a computer matching assessment to the oversight body, prior to conducting a computer match. As stated in the consultation paper, this computer matching assessment should include, for example, a description of the types of records involved, how the computer match is consistent with the requirements of the health sector privacy rules, data security procedures, procedures for the retention and destruction of records, procedures for verifying the accuracy of information prior to taking an adverse action against the individual as a result of the matching procedure, and the business case for conducting the matching procedure.

In addition, we recommend the extension of this requirement to private sector custodians that intend to engage in computer matching activities involving personal health information. The proposed requirements for computer matching would be consistent with Alberta's *Health Information Act*, which states that, before conducting a computer match, a custodian must prepare an assessment and submit it to the Information and Privacy Commissioner of that province. The assessment must describe how the information to be used in the computer match is to be collected and how the information created through the computer match is to be used or disclosed.

What Would Be Included in the Proposed Health Information Privacy Legislation? (MOH page 11)

What types of health information would be included?

We support the proposal to include a broad range of information in the definition of personal health information. We agree that the proposed legislation should not cover personal health information about an individual who has been dead for more than 30 years or recorded information that is more than 100 years old.

We also do not object to the proposal to exclude personal health information related to an individual collected for the purpose of labour negotiations or employment of individuals, providing this type of information is covered by other privacy legislation. It should be noted, however, that this would mean that health information custodians could be subject to two separate privacy schemes – one for personal health information and the other for personal information, including personal health information collected for employment-related purposes.

Similarly, we believe the definition of personal health information should be drafted to ensure that information about the employment and business responsibilities, activities and transactions of individual health service providers is not included. This type of information may be used to objectively assess the quality of provider services and should be considered professional in nature rather than personal health information.

We do not object that the legislation would not apply to truly anonymized information. However, we are concerned the legislation recognize that, in some cases, it may be possible, though unlikely, to identify individuals from anonymous health information through their unique characteristics. It is also possible to de-anonymize seemingly anonymous health information by linking it to publicly available information about individuals. In light of these potential threats to privacy, it is our view that the legislation should include some safeguards for anonymous health information.

Specifically, the legislation should require custodians to ensure that anonymous health information is:

- only used for the purposes for which personal health information may be used under the legislation;
- not combined or linked to any other personally identifiable information; and
- not published in a manner that could be used to identify an individual (e.g., small cells of data).

We understand the rationale for providing specific rules for "quality of care information" and note that specific rules for quality of care information are contained in health information legislation from other jurisdictions. However, we would suggest that records prepared for the purposes of reviewing patient care should be pseudonymized, by replacing all of the personal identifiers (e.g., name, address, health number, etc.) with a special code that can only be linked back to the personal identifiers when it is absolutely necessary to do so.

Who would the rules apply to? (MOH page 11)

We agree that the personal health information privacy rules should apply to a wide variety of individuals and organizations in the health sector, and that these "health information custodians" should be listed in the legislation.

However, in comparing the list of custodians in the consultation paper with the lists contained in previous drafts of the legislation, it is not clear what criteria were used to designate organizations as custodians under the proposed legislation. The Ministry of Transportation, which maintains certain personal health information, was previously designated as a custodian, but was excluded from the list of custodians in this consultation paper. One might assume this exclusion was the result of the narrowing the scope of the legislation to focus more closely on the health sector. However, insurance companies have also been removed from the list of custodians. Other organizations which one might reasonably think are not part of the health sector, such as the Ministry of Consumer and Commercial Relations, continue to be included in the list of custodians. The rationale for including individuals and organizations in the list of custodians needs to be defined in the legislation. For example, insurance companies clearly utilize vast quantities of personal health information and should be listed as a health information custodian.

How Would the Proposed Health Sector Privacy Rules Protect Personal Health Information? (MOH page 14)

We strongly endorse the proposal for the health sector privacy rules to protect personal health information by setting specific limitations on the types of information that may be collected, used, and disclosed. In general, we agree with the key features outlined in the consultation paper on how personal health information should be protected.

Individuals should have to give their consent before personal health information is disclosed. We would add that the exceptions to this general rule should be limited as well as specific. Personal health information should only be collected, used, or disclosed if other information (e.g., aggregate information or registration information) would not serve the purpose. Custodians should only be permitted to collect, use, and disclose the necessary amount of personal health information. Custodians should have a duty to protect the individual's identity to the greatest extent possible and to maintain the confidentiality and security of personal health information. The rules for the collection, use, and disclosure of personal health information should apply to all individuals employed by or in the service of the custodian. Information managers should be contractually bound to adhere to the requirements of the legislation. We agree there should be an independent oversight body responsible for reviewing complaints, auditing information practices, and ensuring compliance with the legislation.

We also agree that the custodian should be required to take reasonable steps to ensure that the privacy protection provisions of the health sector rules are respected when personal health information is disclosed to a non-custodian within the province, or used and disclosed outside of the province. One approach would be to require custodians to contractually bind recipients of personal health information to the requirements of the legislation.

It is our understanding that the federal *Personal Information Protection and Electronic Documents Act* will apply to personal health information that is transferred from Ontario to another province for commercial purposes. However, the federal legislation does not provide any protection for personal health information that is transferred from Ontario to another province for non-commercial purposes or to another country for any purpose.

Individuals and organizations in Ontario that are not designated custodians under the health sector privacy rules will be covered under public or private sector legislation. However, the various pieces of legislation incorporate different privacy standards.

Therefore, to ensure an adequate level of privacy protection, recipients of personal health information (within or outside the province) that are not custodians under Ontario's legislation should be contractually bound to comply with the requirements of the health sector privacy rules. In addition, custodians that use personal health information outside of the province should also be required to comply with the legislation.

What Rights Would Individuals Have? (MOH page 17)

We generally agree with the proposed rights of individuals under the proposed health information privacy legislation. We strongly believe individuals should have the right to:

- consent to the disclosure of their personal health information, except in the limited circumstances set out in the legislation;
- access and request correction of their health records, with limited and clearly defined exceptions;
- challenge a refusal to provide access; and
- complain about the custodian's compliance with the legislation to an independent oversight body.

In addition to the rights outlined in the consultation paper, we believe individuals should have the right to consent to the collection and use of their personal health information, except in limited circumstances. Also, where a custodian refuses a request to correct personal health information, individuals should be able to request that a statement of disagreement be attached to the record, as well as to challenge a custodian's refusal to correct personal health information to the oversight body. This would be consistent with the rights of individuals under Alberta's *Health Information Act* and the rights of individuals under Ontario's public sector privacy legislation.

We also agree that the legislation should place limits on the collection and use of the health number, comparable to those that currently exist under the *Health Cards and Numbers Control Act*.

What would the rules be for giving consent? (MOH page 17)

We agree that the health sector privacy rules should set out the criteria for informed consent for the collection, use, and disclosure of personal health information. However, we believe the proposed rules also should set out precisely what information should be included in the consent, rather than simply suggesting what information might be included. Specifically, the consent should include:

- the identity of the person who will collect, use, disclose, or receive the personal health information;
- the purpose of the collection, use, or disclosure;
- the nature and extent of the personal health information to be collected, used, or disclosed;

- the potential consequences of giving or withholding consent to the collection, use, or disclosure; and
- if the personal health information will be used or disclosed outside Ontario, that the privacy protections may differ outside the province.

In addition, the consent should include a statement that the individual may specify a time after which the consent will cease to be effective and a statement that the individual may revoke the consent at any time.

Alberta's *Health Information Act* sets out what must be included in a consent. We believe it would be useful if Ontario's health sector privacy rules specified what should be included in a consent.

What would happen when an individual is unable to give consent? (MOH page 18)

Generally, we support the proposed framework to address situations where the individual is not capable of providing consent for the collection, use, and disclosure of personal health information. The legislation should set out the types of individuals who can make a decision on behalf of an incapable person. We concur that in making decisions on behalf of another individual, the wishes, values, and beliefs of the individual should be considered. Parents, or another person who is lawfully entitled to act in place of a parent, should be able to provide consent to the collection, use, and disclosure of personal health information for children who are not capable of providing consent.

It is our view that the legislation should not create special rights for substitute decision makers. Instead, a substitute decision maker should be permitted to exercise, on behalf of the individual, any of the rights that the individual may exercise under the legislation.

What rights would individuals have to access and request correction to their personal health records? (MOH page 19)

We are pleased with the proposed approach to provide individuals with the right of access to, and correction of, their own personal health information. We agree that exceptions to these general rights should be "very limited." Decisions to refuse to grant access or correction should be appealable to the independent oversight body. As suggested in the consultation paper, although the legislation may set out a formal process for obtaining access to personal health information, this should not replace other informal processes for obtaining access.

With respect to fees, we recognize that an organization may incur some expense in responding to a request for access. Nevertheless, our preference would be for organizations not to require individuals to pay fees for accessing their own personal health information. At a minimum, any fees that may be charged under the legislation should not present a barrier to access. If fees are permitted under the legislation, we agree that rules for determining the level of fees and conditions for waiving them should be set out in the legislation or in regulations.

We also agree that parental rights of access should be stipulated in the legislation, except in situations where they are not appropriate, as outlined in the consultation paper.

With respect to accuracy, we would suggest that where the custodian refuses to correct or amend personal health information, the individual should have the right to attach a statement of disagreement to the record, and to appeal this decision to the oversight body. In some cases, a statement of disagreement is not sufficient to protect individuals from any adverse consequences of the use and disclosure of inaccurate personal health information. For this reason, individuals must be able to challenge a refusal to correct or amend personal health information to the oversight body.

In addition, when a statement of disagreement is attached to a record, we suggest that the custodian should be required to provide a copy to: 1) any person to whom the custodian has disclosed the record in the year preceding the applicant's request for an amendment or correction, and 2) anyone to whom the custodian subsequently discloses the information. This would also be consistent with the requirements of the health information protection legislation in Alberta.

What Responsibilities Would Health Information Custodians Have? (MOH page 21)

We believe the responsibilities of health information custodians outlined in the consultation paper are appropriate. As proposed, custodians should be required to:

- take reasonable steps to establish and maintain administrative, technical and physical safeguards and practices;
- be open about their information management practices;
- establish written policies regarding the retention and disposal of records of personal health information; and
- designate a contact person.

The type of openness required under the proposed privacy rules for the health sector is one of the most important components of privacy protection. As noted earlier in our discussion about recording unanticipated disclosures, openness is a prerequisite for individuals to exercise their rights under the legislation. For example, before individuals can access or request correction of their own personal health information or lodge a complaint, they need to be able to obtain information about procedures for accessing and correcting their own personal health information and procedures for challenging the organization's compliance with the privacy principles.

We also agree that the proposed privacy rules for the health sector should require custodians to designate a contact person. This will not only facilitate the custodian's implementation and compliance with the privacy rules, but also will help individuals to exercise their rights by providing a point of contact with the organization regarding privacy matters. The designation of one or more individuals who are responsible for compliance with the legislation fosters accountability, which is one of the privacy principles of the CSA Model Code and the federal *Personal Information Protection and Electronic Documents Act*.

Due to the sensitivity of personal health information, we support the idea of requiring custodians to prepare a privacy impact assessment under certain circumstances. Alberta's *Health Information Act* contains such a requirement. However, we are mindful that such a provision should not be administratively burdensome to the custodians. Accordingly, we believe the privacy rules for the health sector should define when such an assessment is appropriate.

What Rules Would Be In Place For Collecting, Using and Disclosing Personal Health Information? (MOH page 23)

We support the proposed general rules for collection, use, and disclosure of personal health information. Specifically, health information custodians should only be permitted to collect, use, and disclose personal health information if other information would not serve the purpose. They should only collect as much information as necessary for the purpose and, to the extent reasonably possible, they should take steps to protect the identities of individuals. Informed consent for the collection, use, and disclosure of personal health information should be the norm, except in the limited circumstances specified in the legislation.

What rules would cover collection of personal health information? (MOH page 23)

As suggested in the consultation paper, the collection of personal health information should be limited to that which is necessary for a lawful purpose related to a function or activity of the custodian. However, we do not agree that collection of personal health information also should be allowed simply because it is expressly permitted by a specific law. Unless it is required by law, it is our view that the collection of personal health information should be limited to that which is necessary for the lawful purpose for which it is being collected. This would be consistent with the restrictions on collection imposed under the *Personal Health Information Act* of Manitoba.

We agree that custodians should be required to take reasonable steps to inform the individual of the purposes for which the information is being collected, at the time of collection, or as soon as possible afterwards. As we noted earlier, openness and transparency of practice is critical to enable individuals to exercise their rights under the proposed privacy rules for the health sector. Specifically, we believe that, at the time of collection, custodians should be required to inform individuals about the following:

- the purposes for collecting personal health information;
- anticipated uses and disclosures of personal health information;
- where consent is required for the collection, use, or disclosure of personal health information, that individuals may specify a time after which their consent is no longer valid;
- where consent is required for the collection, use, or disclosure of personal health information, that individuals may, at any time, revoke their consent in writing;
- the procedures for requesting access to and/or correction of personal health information;

- that a copy of the organization's policies and procedures regarding the collection, use, and disclosure of personal health information will be provided upon request;
- that a copy of the documentation about unanticipated uses and disclosures of personal health information will be provided upon request;
- the administrative, technical, and physical safeguards relating to the confidentiality and security of the personal health information; and
- who to contact to ask questions about the collection; to request access or correction of personal information; and to complain to about the collection, use, and disclosure of personal health information.

We also agree that personal health information should have to be collected directly from the individual to whom the information relates, except in limited and specific circumstances defined in the health sector privacy rules.

What rules would cover use and disclosure of personal health information?

(MOH page 24)

We agree that the legislation should require that personal health information only be used for certain purposes. In our view, some of the permitted uses without consent could be narrower. For example, one of the proposed rules is that information may be used if it may be disclosed, or is required to be disclosed, to the custodian under the health sector privacy rules. Unlike the other proposed uses, this particular use is not tied to a specific purpose. It seems to imply that if the information can be disclosed to the custodian, the custodian may use it for any purpose. In our view, the custodian to whom the information is disclosed should be able to use the personal health information only for the purpose for which it was disclosed to the custodian. In addition, we suggest narrowing the permitted use of personal health information for the purpose of educating persons employed by or in the service of the custodian and who provide health care. We believe this type of use should be permitted only with the knowledge and consent of the individual.

We agree that custodians should be required to identify expected uses and disclosures of an individual's personal health information. But, rather than just being required to explain anticipated uses and disclosure when asked, we suggest that custodians should be required to inform individuals about anticipated uses and disclosure of personal health information before or at the time of collection. This could include, for example, informing individuals that the custodian intends to use the personal health information to create anonymous, pseudonymous, or aggregate health information to be used for secondary purposes, such as research.

However, if as suggested in the consultation paper, custodians are only required to explain anticipated uses and disclosures when asked, we believe that, as a minimum, the custodian should be required to inform individuals, at the time of collection or before, that information about the anticipated uses and disclosures of personal health information will be made available to them upon request.

We agree that before using or disclosing personal health information, custodians should be required to take reasonable steps to ensure the information is accurate, complete, and not misleading. The requirement to ensure the accuracy of personal information is an important fair information practice. If there is no requirement for accuracy, then inaccurate, incomplete, or out-of-date information could proliferate throughout a number of databases and be used to make decisions that will adversely affect the individual. We are pleased to see this standard of accuracy incorporated into the proposed health sector privacy rules.

As suggested in the consultation paper on the health sector privacy rules, the legislation should prohibit the use and disclosure of personal health information for marketing purposes without the individual's consent. We are not opposed to the use of certain personal information for charitable fundraising activities by health care facilities, providing that:

- the use and disclosure of personal health information is limited to name and address;
- individuals are notified each time they are contacted for the purpose of raising funds that they may opt out of the fundraising list; and
- reasonable steps are taken to ensure that individuals who may not want to be contacted by the health care facility (e.g., due to the sensitive nature of the circumstances) are not contacted.

We agree that guidance as to how to address "very sensitive" circumstances is required. Our preference would be to require "opt in" (e.g., express consent) for such situations, rather than opt out.

Additionally, in all other circumstances, our preference would be for custodians to provide individuals with an opportunity to opt out of the use of their personal information for fundraising activities at the time when their personal information is first collected. However, at a minimum, individuals should be provided with this opportunity when they are first contacted for this purpose and on every occasion thereafter.

We also agree that the proposed health sector privacy rules should protect health numbers, as currently provided for under the *Health Cards and Numbers Control Act*.

What additional rules would cover disclosure of personal health information? (MOH page 25)

We are pleased that the starting point for the health sector privacy rules will be that personal health information will only be disclosed with the consent of the individual, and that the exceptions to this general rule will be set out in the legislation. We would add that, in accordance with fair information practices, the exceptions to this general rule should be as limited and specific as possible.

In our view, personal health information should only be disclosed for health care purposes, with the consent of the individual. This would be consistent with our comments regarding the lock box provision, which has been omitted from the proposed rules. We note that in some cases, it may be reasonable for custodians to imply consent to share personal health information with other custodians who are directly involved in providing health care to the individual. However, consent must never be implied when individuals have expressed a desire not to have their personal health information disclosed without their explicit consent.

We agree that the limited circumstances when personal health information may be disclosed without consent need to be set out in the legislation. It should also stipulate the circumstances when notice of such disclosures is required. We believe there are some circumstances (e.g., when personal health information is disclosed for the purpose of determining or verifying eligibility of an individual for publicly funded benefits) when custodians must ensure that the individual is informed of the disclosures.

We question the scope of the proposed exception to the consent requirement for the purpose of determining or verifying eligibility to receive health care or other benefits. Under Saskatchewan's *Health Information Protection Act*, the Minister of Health may disclose registration information to certain organizations for this purpose. Accordingly, unless there is a clear rationale for a broader exception, we would suggest that this exception be narrowed to permit disclosure only by specific custodians (e.g., the Minister of Health and Long-Term Care), to limit the disclosure to specific personal health information (e.g., registration information), and to permit the disclosure only to specific recipients (e.g., other government institutions).

We agree that health facilities should be able to continue to disclose a limited amount of information in response to inquiries, except where individuals have requested that no information be disclosed. We would add that before such information is disclosed, custodians should be required to notify individuals that they may request that no information be disclosed in response to inquiries.

We support the inclusion of provisions to allow custodians to disclose certain information about people who have died. Although Ontario's public sector privacy legislation does not provide any special right of access to the personal information of a deceased person, Quebec's private sector legislation grants a broad range of access to information relating to the cause of death contained in the deceased's health information records. Public sector privacy legislation from Alberta and Manitoba also contains provisions which recognize the importance of disclosing personal information in compassionate circumstances.

We recommend the narrowing of the exceptions to the consent requirement related to improving health or the delivery of health services, or to protecting the health of people in a community. For example, it is not clear why disclosures to public health officials for the purpose of public health promotion is permitted without the consent of individuals. In the absence of evidence to suggest that the activities of this custodian would be adversely affected by requiring consent, we believe consent should be required when such disclosures take place.

We agree that custodians should be permitted to disclose personal health information for certain approved health screening programs designated in the regulations. We are pleased that, under the proposed legislation, individuals will be informed that they may opt out of participating in such screening programs.

We are not opposed to an exception to the consent requirement to prevent harm. However, we believe the scope of the exception for the disclosure of personal health information to the head of a penal or other custodial institution, or to the head of a psychiatric facility in which the individual is being lawfully detained should be narrowly defined. We understand that on occasion, personal health information may be essential to assist an institution or facility in managing an individual's physical or mental health, placement into custody or detention, or release into the community. However, such disclosure should be limited to only information that is necessary to make an informed decision.

We understand the Minister of Health and Long-Term Care may require access to certain information for the purposes of administering and managing the publicly funded health care system. Under the proposed framework, the Minister may require custodians to disclose personal health information or may require a custodian to disclose personal health information to another organization for these purposes. However, in our view, the framework being proposed is too broad. In addition, where the health service is funded, in whole or in part, by the Ministry of Health and Long-Term Care, there is no process for reviewing the directions to disclose issued by the Minister.

We recommend stronger privacy safeguards be incorporated into this proposed framework governing the disclosure of personal health information for the purposes of administering and managing the health system. First, there need to be limits on what personal health information a custodian may be directed to disclose. Second, the persons or classes of persons to whom the information may be disclosed should be set out in legislation rather than in regulations. Third, the entire process needs to be open to review by the independent oversight body. Specifically, regardless of who funds the health services provided by custodians, they should be permitted to refuse the direction to disclose and to ask for a review of the refusal by the independent oversight body.

We do not object to the proposed rules for disclosing personal health information for use in proceedings.

How Would the Health Sector Privacy Rules Be Administered and Enforced? (MOH page 31)

We agree that there should be an independent oversight body and the roles of that body should be set out in the legislation. We support the proposed legislation including offences and penalties for breaching the requirements of the legislation. We also agree that there should be a single oversight body responsible for compliance with all provincial privacy legislation.

The proposal for the broad private sector privacy legislation indicated that, similar to the federal legislation, "whistleblower protection" was being contemplated. We believe there may be merit in similar provisions under the health sector privacy rules.

What role would an oversight body play? (MOH page 31)

We emphatically endorse the statement in the consultation paper indicating that the oversight body should have a significant role in enforcing the health sector privacy rules. We support the proposal that the oversight body have the necessary enforcement powers including the power to investigate complaints, enter premises and examine relevant records, and issue binding orders.

The privacy compliance enforcement approach that is proposed in the consultation paper is consistent with that which is already in place for Ontario's public sector privacy legislation. We support this approach and note that this approach is somewhat different from the business regulation enforcement model set out in the consultation paper on the proposed private sector privacy legislation. In accordance with the goal of having only one oversight body, we would suggest that all privacy legislation should be based on the compliance enforcement principles which form the basis for the existing public sector privacy legislation in Ontario.

In addition to the roles of the oversight body set out in the consultation paper, we would also suggest that the oversight body be authorized to conduct assessments and offer comment on the privacy impact of programs and proposed legislation. Such reviews can be an effective tool in raising awareness of privacy on the part of both the public and health information custodians.

The oversight body should also be empowered to conduct public education programs and to provide information about the legislation and the roles and activities of the oversight body under the legislation.

Finally, the oversight body should be given express powers to engage in or commission research into any matters affecting the understanding or carrying out of the purposes of the legislation; to give advice and recommendations of general application to custodians on matters respecting their rights or obligations under the legislation; and to receive representations from the public concerning the operation of the legislation. These powers are comparable to those under the existing public sector privacy legislation.

What would happen if a person had a complaint? (MOH page 31)

We agree that the oversight body should receive complaints about:

- a custodian's information practices;
- any alleged contravention of the legislation; or
- a refusal to provide access to or to attach a statement of disagreement to a personal health record, in cases where a request to correct or amend personal health information has been refused.

In addition, the oversight body should be able to receive complaints about a direction to disclose personal health information issued by the Minister of Health and Long-Term Care.

As suggested in the consultation paper, the oversight body should have the discretion to refuse to investigate a complaint not taken initially to the custodian. We support the approach that the oversight body could conduct a review of the information practices of a custodian if there are reasonable grounds to believe that the custodian is not complying with the legislation. We also agree that the oversight body should have the power to issue binding orders that would require compliance with the legislation and that a wilful failure to comply with such an order should be an offence under the legislation.

When would the personal health information privacy legislation be reviewed? (MOH page 33)

We believe that legislative reviews are useful and we endorse the idea of a review no later than three years after it comes into force.

What other Acts would be amended as a result of the proposed personal health information privacy legislation? (MOH page 33)

We recognize that there may be the need to amend certain pieces of legislation as a result of proposed personal health information privacy legislation. We would not object to the repeal of the *Health Cards and Numbers Control Act* **providing** that its provisions were first incorporated into the proposed legislation.

Conclusion

In conclusion, we would like to commend the Ministry of Health and Long-Term Care for its persistent efforts to implement privacy rules for the health sector. We also would like to recognize the considerable effort that has gone into consulting with the various stakeholder groups on this initiative. We understand that the proposed privacy rules, in many cases, reflect compromises that have been made to satisfied the divergent needs of stakeholder groups.

While being supportive of the overall objective, the IPC, as noted in this submission, has two major areas of concern regarding the proposed privacy rules for the health sector. Our first concern is about the timing of this initiative. Our preference would be for the Government of Ontario to proceed with the implementation of broader private sector privacy legislation now, and to have the health sector privacy rules developed within the context of that legislation. However, as these two initiatives seem to be proceeding simultaneously, at this point in time, it is not clear how the health sector privacy rules will compare to the privacy rules that will eventually be implemented for other sectors. Also, since the health sector privacy rules do not generally conform to the standard CSA Model Code, it is not clear how these rules will be harmonized with the broader private sector privacy rules, or with the federal private sector privacy rules as set out in the federal *Personal Information Protection and Electronic Documents Act*.

Our second major concern relates to the proposed broad disclosures of personal health information that are permitted under the rules, without the consent of individuals. Specifically, we are concerned about the elimination of the lock box provision, which would have allowed individuals to prohibit the disclosure of personal health information for the purposes of providing health care. In addition, although we recognize that an attempt has been made to limit permitted disclosures without consent, it is our view that further definition needs to be done in this respect. Accordingly, we have made a number of suggestions to reduce the number and narrow the scope of the disclosures that are permitted without the consent of the individual.

We also believe that the framework for the disclosures of personal health information for the purposes of administering and managing the health system should be narrower and more specific than that which is being proposed in the consultation paper. In addition, it is our view that all disclosures of personal health information that are directed by the Minister of Health and Long-Term Care should be subject to review by the independent oversight body.