

ASSOCIATION
MÉDICALE
CANADIENNE



CANADIAN
MEDICAL
ASSOCIATION

1867, prom. Alta Vista Dr., Ottawa ON K1G 3Y6
(613) 731-9331 • 1 800 267-9703
Fax/Télec. : (613) 731-1755 • www.cma.ca

BRIEF

.....
MÉMOIRE

“Putting Patients First”

Comments on Bill C-6

(Personal Information Protection and Electronic Documents Act)

Submission to the Senate Standing Committee on Social Affairs, Science and Technology

Nov. 25 1999
Ottawa, Ontario

For further information, contact
CMA's Public Affairs Directorate : 1 800 267-9703

Leadership for Physicians... Health for Canadians

..... *Leadership pour les médecins... Santé pour les Canadiens*



The Canadian Medical Association (CMA) is the national voice of Canadian physicians. Founded in 1867, CMA's mission is to provide leadership for physicians and to promote the highest standard of health and health care for Canadians.

On behalf of its members and the Canadian public, CMA performs a wide variety of functions, such as advocating health promotion and disease/accident prevention policies and strategies, advocating for access to quality health care, facilitating change within the medical profession, and providing leadership and guidance to physicians to help them influence, manage and adapt to changes in health care delivery.

The CMA is a voluntary professional organization representing the majority of Canada's physicians and comprising 12 provincial and territorial divisions and 43 affiliated medical organizations.

Table of Contents

	EXECUTIVE SUMMARY	i.
I.	INTRODUCTION	1
II.	RATIONALE AND SCOPE OF BILL C-6	2
	A. Rational of Bill C-6	2
	B. Scope - Application to Medical Records	3
	C. Scope - Government Excluded	5
III.	CONSIDERATIONS REGARDING PATIENT PRIVACY AND CONFIDENTIALITY: VERSUS COMMERCIAL CONTEXT	5
	A. CMA's Opinion	5
	B. Public Opinion	7
	C. The Advisory Council Report	7
	D. The Approach in Bill C-6	8
	E. Conclusion	8
IV.	SPECIFIC COMMENTS ON BILL C-6 FROM THE PERSPECTIVE OF CMA'S HEALTH PRIVACY CODE	10
	A. General	11
	B. Primacy of the Therapeutic Purpose	11
	C. Knowledge of Purpose Prior to Collection	13
	Bill C-6	13
	CMA Health Information Privacy Code	14
	D. Use Without Knowledge Or Consent	15
	Bill C-6	15
	CMA Health Information Privacy Code	16
	The Advisory Council Report	17
	E. Disclosure Without Knowledge Or Consent	18
	Bill C-6	18
	CMA Health Information Privacy Code	18
	F. Consent	18
	Bill C-6	18
	CMA Health Information Privacy Code	18
	The Advisory Council Report	17
	G. Information Flow within Organizations	19
	Bill C-6	19
	CMA Code	20
	H. Information Protected	19
	Bill C-6	19
	CMA Code	20
	The Advisory Council Report	17
	I. Individual Access	20
	Bill C-6	20
	CMA Code	20
	J. Accuracy and Amendment	20
	Bill C-6	20
	CMA Code	21
	K. Sensitivity	20
	Bill C-6	20
	CMA Code	20
V.	CONCLUSIONS	21
VI.	SUMMARY OF RECOMMENDATIONS	22

Executive Summary

CMA commends the federal government for taking this important first step that begins the debate on privacy and the protection of personal information. The issues are complex and the interests at stake significant. CMA welcomes the opportunity to provide comments on Bill C-6 and hopes that its input will strengthen the Bill by ensuring that patient privacy and the confidentiality of medical records are adequately protected.

CMA's chief concern with Bill C-6 is the inadequacy of its provisions to protect the right of privacy of patients and the confidentiality of their health information. The right of privacy encompasses both the right to keep information about ourselves to ourselves if we so choose and to exercise control over what subsequently happens to information we confide in trust for the purpose of receiving health care. In recent years, this right, and the ability of physicians to guarantee meaningful confidentiality, have becoming increasingly threatened.

Computerization of health information facilitates easy transfer, duplication, linkage and centralization of health information. Captured in electronic form, patient information is potentially more useful for the purpose of providing care. However, thus captured, it also becomes much more valuable and technically accessible to various third parties -- private and public, governmental and commercial -- wishing to use this information for other purposes unrelated to providing direct care. An additional concern is that the demand for health information, referred to by some commentators as 'data lust', is growing, partly as a consequence of 'information hungry' policy trends such as population health. There is also a disturbing tendency toward 'function creep', whereby information collected for one purpose is used for another, often without consent or even knowledge of the individual concerned and without public knowledge or scrutiny.

Furthermore, initiatives concerning health information technology tend to be dominated by those who seek access to this information for secondary purposes. From this perspective, privacy may appear less as a fundamental right than as a hindrance or even roadblock. As we move further into the information age there is some danger that we will become so spell-bound by the promise of information centralization and database linkages that we lose sight of the patients who confided this information or reduce them to impersonal 'data subjects'.

To avoid this danger and the allure of the technology we need to ground the application of information technology and practices in well-tested, enduring principles. We need to put privacy first rather than treat it as a nuisance or impediment. Rules and regulatory regimes concerning health information should be based on the principle of patient privacy because ultimately health information technology is not about ‘bits and bytes’ or ‘data’ or even ‘data subjects’ but about patients, and patients deserve to be treated with respect and dignity and to have their wishes and choices valued and respected.

If we are to put patients first the right of privacy must be given primacy in rules concerning health information. This does not mean that this right is absolute. What it does mean is that the burden of proof must rest with those whose purposes, however compelling they may be, encroach upon the right of privacy. It means that we value patient privacy at least enough to demand explicit justification of any proposal that would diminish privacy.

Bill C-6 begins with the right premise: that “rules to govern information collection, use and disclosure” should recognize the “right of privacy”. However, it fails to recognize the special nature of health information and to tailor its provisions accordingly. In consequence there is confusion and uncertainty about Bill C-6's application to health care. Even more seriously, however, Bill C-6 fails to recognize that health information requires stronger or greater privacy protection than other types of information.

The inadequacy of Bill C-6 for health care is not surprising because clearly it was not drafted with health information in mind. Rather, it is written from the perspective of encouraging commerce. It appears to have access to information as its dominant value. The world of health care is very different from that of commerce and consequently requires distinct rules that are more protective of privacy. Confiding information to your physician under the trust of the patient-physician relationship is not on par with giving your address to a salesclerk when you purchase a toaster or rent a movie. Health information is special by nature. Canadians know this. In a recent Angus Reid poll commissioned by CMA Canadians told us loudly and clearly that they regard their health information as especially sensitive.

However, the obvious sensitivity of health information is not the only thing that makes it special and in virtue of which it warrants distinct rules to strengthen privacy protection. It is important to recognize that this information is typically collected under the trust patients vest in their physicians. Patients confide their information for the purpose of receiving care and in the expectation that it will be held in the strictest confidence. This purpose, and the preservation of this trust, should be given primacy in rules concerning health information. It is also important to recognize that the trust under which patients confide in their physicians is fundamental to the patient-physician relationship. If patients can not trust their physicians to protect their information and keep it secret they will not confide it as freely as they do. In consequence, the ability of physicians to provide the care needed would be severely diminished.

Rules relating to health information must be developed in recognition of its special nature and the circumstances of trust and vulnerability in which it is initially collected or confided. Patients confide in their physicians for the purpose of receiving care. The potential that the information thus confided may subsequently be used for other purposes must not impede the therapeutic purpose or diminish the trust and integrity of the patient-physician relationship.

In recent years the secondary use of information for purposes other than those for which it was collected has been increasing without adequate oversight or public knowledge. This ‘function creep’ undermines the trust of patient-physician relationship. Collection and use beyond the therapeutic context and for purposes unrelated to the provision of direct care should be subjected to rigorous scrutiny before they are permitted to occur. To the extent that they are permitted to occur without patient consent they should be explicitly authorized in legislation to ensure transparency and adequate oversight.

Putting patients first means ensuring that health information, in all but exceptional and justifiable circumstances, is used *only* under the strict control of the patient. The patient must be able to exercise control through voluntary, informed consent. Moreover, a distinction must be made between a patient’s right to know what can or must happen to health information and the right to consent to such use. Bill C-6 permits the collection, use and disclosure of information without knowledge or consent on grounds such as expediency, practicality, public good, research, offence investigation, historic importance and artistic purpose. The laxness and breadth of these exemptions as applied to health information is unacceptable. These uses, without the patient’s consent (or even knowledge), reduce the patient to a means to someone else’s end, however worthwhile that end may be. Moreover, the absence of consent (or even knowledge) undermines the integrity of the patient-physician relationship and has the potential to erode the trust patients have in their physicians - a trust that is essential to patients’ willingness to provide the complete information needed to provide them with care.

CMA has developed and adopted a Health Information Privacy Code (Appendix A) in recognition of the special nature of health information and to give primacy to patients and to the right of privacy. This Code begins from the same starting point as Bill C-6, the Canadian Standards Association (CSA) Code which the Bill includes as Schedule 1. However, unlike Bill C-6, the CMA Code tailors the CSA Code to the specific circumstances of health information. The CMA Health Information Privacy Code, therefore, is able to address issues specific to health information that Bill C-6 either fails to address or, even worse, exacerbates.

In light of the clear deficits in Bill C-6 and the inadequate protection of patient privacy and health information confidentiality, CMA urges this committee to accept the recommendations put forward in this brief to strengthen the Bill’s provisions for protecting privacy and to accept the amendment (Appendix B) CMA has prepared to give effect to these recommendations. CMA believes that Canadians desire and deserve no less than this as concerns the right of privacy with respect to health information.

I. Introduction

The Canadian Medical Association is the national voice of Canadian physicians. Our mission is to provide leadership for physicians and to promote the highest standard of health and health care for Canadians. The CMA is a voluntary professional organization representing the majority of Canada's physicians and comprising 12 provincial and territorial divisions and 43 affiliated medical organizations. On behalf of its 46,000 members and the Canadian public, CMA performs a wide variety of functions, including addressing the emerging issue of electronic health information and confidentiality and privacy. It is in this capacity that we present our position on Bill C-6, *The Personal Information Protection and Electronic Documents Act*.

CMA commends the federal government for taking this important first step of beginning the debate on privacy and the protection of personal information. The issues are complex and the interests at stake significant. CMA welcomes the opportunity to provide comments on Bill C-6 and hopes that its input will strengthen the Bill by ensuring that patient privacy and the confidentiality of medical records are adequately protected. In preparing this brief CMA has had the benefit of the final report of the federal Advisory Council on Health Infostructure, *Canada Health Infoway: Paths to Better Health: Final Report*. ("Advisory Council Report") Where appropriate, CMA cites the findings contained in the Report.

CMA wishes to underscore the key themes of its brief:

- A. Health information is special by its nature. Rules relating to health information must be developed in recognition of its special nature. Ensuring protection of privacy and confidentiality of the patient record must take precedence over other considerations. Bill C-6 fails to do this. Bill C-6 is written from the perspective of encouraging commerce. It appears to have access to information as its dominant value. The world of health care is very different from that of commerce and consequently requires distinct rules.
- B. Typically, health information is confided in the context of the therapeutic relationship and under the trust upon which this relationship is built. Rules concerning health information -- and in particular its collection, disclosure and use for purposes unrelated to the provision of direct care -- must be consistent with the expectations of patients about confidentiality and must not exploit the trust patients have in their physicians or compromise the ability of physicians to earn and maintain this trust.
- C. Health information must, in all but exceptional and justifiable circumstances, be used *only* under the strict control of the patient. The patient must be able to exercise control through voluntary, informed consent. Moreover, a distinction must be made between a patient's right to know what can or must happen to health information and the right to consent to such use. Bill C-6 permits the collection, use and disclosure of information without knowledge or consent on grounds such as expediency, practicality, public good, research, offence investigation, historic importance and artistic purpose. The laxness and breadth of these exemptions as applied to health information is unacceptable. These uses, without the patient's consent (or even knowledge), reduce the patient to a means to someone else's end, however

worthwhile that end may be. Moreover, the absence of consent (or even knowledge) undermines the integrity of the patient-physician relationship and has the potential to erode the trust patients have in their physicians - a trust that is essential to patients' willingness to provide the complete information needed to provide them with care.

- D. The root of most of the problems in applying Bill C-6 to health care information is its failure to distinguish among purposes for the collection, use and disclosure of health information. In particular, the Bill fails to distinguish between the primary purpose, which is to deliver care to and for the benefit of an individual patient, and secondary purposes, which are not for the direct benefit of the patient (and indeed may even use the patient's information to his or her detriment). Provisions to protect privacy should give recognition to the difference between these purposes and should not hinder the ability of physicians and others to provide care consistent with the patient's wishes. Moreover, the Bill has no effective mechanism to distinguish legitimate purposes, which should be permitted, from illegitimate purposes, which should not, notwithstanding the limitation to "purposes that a reasonable person would consider are appropriate in the circumstances" in Section 5(3).
- E. In recent years the secondary use of information for purposes other than the purpose for which it was collected has been increasing without adequate oversight or public knowledge. This 'function creep' undermines the trust of patient-physician relationship. Collection and use beyond the therapeutic context and for purposes unrelated to the provision of direct care should be subjected to rigorous scrutiny before they are permitted to occur. To the extent that they are permitted to occur without patient consent they should be explicitly authorized in legislation to ensure transparency and adequate oversight.

This Brief will first look at the apparent rationale of Bill C-6 and its potential application to health information. The brief will then describe why CMA considers health information to be special in nature and worthy of special protection. Finally, the brief reviews the difference in approach between Bill C-6 and CMA's Health Information Privacy Code to illustrate that Bill C-6 provides inadequate protection to patient privacy and medical confidentiality.

II. Rationale and Scope of Bill C-6

A. Rationale of Bill C-6

The driving force behind Bill C-6 is the support and promotion of electronic commerce. The second part of the Bill is devoted to permitting electronic versions of documents and signatures to be legitimate or 'originals' if the provisions of the Act are followed. Part 2 of the Bill is quite distinct from Part 1 and both parts could stand alone as separate pieces of legislation.

Part 2 simply allows electronic versions of documents and signatures to be recognized as legitimate. On its face, this has little to do with the protection of personal information except to the extent that storage of documents in electronic form provides greater ability to access, link and merge information. Certainly, the Bill appears to draw on this connection by including, in its statement of purpose, the provision of a right of privacy in an era in which technology increasingly facilitates the collection and free flow of information.

Part 1 concerns all forms of personal information, electronic and otherwise. It gives some protection to personal information by requiring consent in some instances. In CMA's view, a fundamental difficulty with Part 1 and with the Bill in general is that its goal is to promote commerce and thus all information is implicitly considered as falling within the 'commercial' realm. In the case of health information this is surely not the case or the only consideration. Moreover, this creates a clash of values when applied to a health care system that is a public system. The Advisory Council Report takes a firm stand on this issue and states that legislation respecting the privacy protection of health information, "should also contain a clear prohibition against all secondary commercial use of personal health information." Moreover, Bill C-6 fails to distinguish and prioritize different purposes for collecting, using and disclosing information and in doing so treats all purposes as more or less equal and subject to the same rules. CMA takes a quite a different view when it comes to health information and will expound its view throughout this brief.

B. Scope - Application to Health Records

CMA has argued from the outset that C-6 (and its predecessor C-54) will apply to some health information. This view now appears to be widely accepted. Nevertheless, it is unclear as to what extent Bill C-6 will apply to health records. The full name of the Act states, in part:

An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in *certain circumstances*

What are these circumstances?

Section 4(1) states that Part 1 (the part protecting personal information) applies in respect of personal information that:

- (a) the organization collects, uses or discloses in the course of commercial activities; or**
- (b) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.**

The definition of commercial activity given in 2(1) --that commercial activity means any particular transaction, act or conduct or any regular

course of conduct that is of a commercial character@ --is circular and does nothing to clarify uncertainties concerning the Bill's scope.

There are two points to be made here as concerns the application of this Bill to health information. The first concerns clarity around where commercial ends and health care begins. Which health care settings that operate for profit are excluded from the Act? This question speaks to the difficulty of delineating what activity is considered health care and what activity is considered commercial. Moreover the increase in public/private partnerships and joint funding of endeavours within the health care sector, which the government appears to be promoting, may make it increasingly difficult to make this distinction; for example in the area of research.

The second concerns the specification of different regimes for information protection and privacy rights, depending on whether the information is deemed to come under commercial activity. This is clearly not desirable. However, the solution to this problem is not to reduce the privacy rules for all health information to the lowest common denominator but to raise them to a higher level of protection than is afforded commercially acquired information. Subjecting all health information to the regime laid out in the CMA Health Information Privacy Code would achieve this objective.

In preparing this brief CMA has assumed that the Bill will provide a scheme that applies to at least some health information. Three years after it is in force it will apply equally to activities that occur strictly within the provinces, unless there is legislation in the province that is substantially similar to the Bill (see sections 27(2)(b) and 30). No doubt the extent of the federal government's ability to legislate in this area generally will be the subject of extensive debate. However, CMA has no comment on this debate and provides its opinion in the interests of ensuring that the rules that relate to health information are compatible with preserving the integrity of the patient-physician relationship and the protection of patient privacy and health information confidentiality. The federal government has an opportunity to provide Canadians with strong privacy rights in health information. It is incumbent upon the government to do so.

C. Scope - Government Excluded

Bill C-6 expressly excludes a large part of government activity from its ambit. Although government activity is to some extent governed by the *Privacy Act*, R.S.C. 1985, P-21, the rules of this Act provide less protection than those of Bill C-6. Government should subject itself to at least the same rules that it requires of the

private sector in so far as it is a collector and user of information. Indeed, government's practices relating to the collection, storage, merging, transfer and use of health information should be subject to more stringent rules than those found in either the *Privacy Act* or Bill C-6. The Advisory Council Report also calls for the same rules to apply to the public and private sectors, rules that are more stringent than those found in the *Privacy Act* or Bill C-6.

Therefore, CMA recommends:

That, at least in connection with health information, the provisions of the Bill apply equally to the public and the private sectors.

III. Considerations Regarding Patient Privacy and Confidentiality: Medical Context Versus Commercial Context

A. CMA's Position

The world of health care is very different from that of commerce and consequently requires distinct rules that are more protective of privacy. Confiding information to your physician under the trust of the patient-physician relationship is not on par with giving your address to a salesclerk when you purchase a toaster or rent a movie. Health information is special by nature. Canadians know this. In a recent Angus Reid poll commissioned by CMA Canadians told us loudly and clearly that they regard their health information as especially sensitive.

However, the obvious sensitivity of health information is not the only thing that makes it special and in virtue of which it warrants distinct rules to strengthen privacy protection. It is important to recognize that this information is typically collected under the trust patients vest in their physicians. Patients confide their information for the purpose of receiving care and in the expectation that it will be held in the strictest confidence. This purpose, and the preservation of this trust, should be given primacy in rules concerning health information

It is also important to recognize that the trust under which patients confide in their physicians is fundamental to the patient-physician relationship. If patients could not trust their physicians to protect their information and keep it secret they would not confide it as freely as they do. In consequence, the ability of physicians to provide the care needed would be severely diminished.

Rules relating to health information must be developed in recognition of its special nature and the circumstances of trust and vulnerability in which it is initially collected or confided. Patients confide in their physicians for the purpose of receiving care. The potential that the information thus confided may subsequently be used for other purposes must not impede the therapeutic purpose or diminish the trust and integrity of the patient-physician relationship.

In recent years the secondary use of information for purposes other than those for which it was collected has been increasing without adequate oversight or public knowledge. This 'function creep' undermines the trust of patient-physician relationship. Collection and use beyond the therapeutic context and for purposes unrelated to the provision of direct care should be subjected to rigorous scrutiny before they are permitted to occur. To the extent that they are permitted to occur without patient consent they should be explicitly authorized in legislation to ensure transparency and adequate oversight.

Putting patients first means ensuring that health information, in all but exceptional and justifiable circumstances, is used *only* under the strict control of the patient. The patient must be able to exercise control through voluntary, informed consent. Moreover, a distinction must be made between a patient's right to know what can or must happen to health information and the right to consent to such use. Bill C-6 permits the collection, use and disclosure of information without knowledge or consent on grounds such as expediency, practicality, public good, research, offence investigation, historic importance and artistic purpose. The laxness and breadth of these exemptions as applied to health information is unacceptable. These uses, without the patient's consent (or even knowledge), reduce the patient to a means to someone else's end, however worthwhile that end may be. Moreover, the absence of consent (or even knowledge) undermines the integrity of the patient-physician relationship and has the potential to erode the trust patients have in their physicians - a trust that is essential to patients' willingness to provide the complete information needed to provide them with care.

CMA has developed and adopted a Health Information Privacy Code (Appendix A) in recognition of the special nature of health information and to give primacy to patients and to the right of privacy. In commenting on this Code the Advisory Council Report notes:

The Code represents an important contribution to the deliberations of Canadians and legislators on how to safeguard privacy across the health domain.

In his 1998-99 Annual Report, the Federal Privacy Commissioner writes in support of the Health Information Privacy Code:

Legislators looking for guidance on health information privacy law need not re-invent the wheel; the Canadian Medical Association's Health Information Privacy Code is a comprehensive benchmark for achieving a high national level of protection for personal information. The Code could be the basis for drafting legislation. Given the grumblings that the Code sets the bar too high, perhaps some Health Infoway funds should be used to study the impact of its implementation. The patients at the heart of this system deserve no less.

There are several key principles that guided the development of the Health Information Privacy Code and upon which it is based:

1. The provision of health care to all Canadians irrespective of social circumstances or health status is a highly regarded value in Canadian

society. The system is publicly funded and universally accessible.

2. The right of privacy is fundamental to a free and democratic society.
3. Rules relating to health information must recognize its special nature. Health information has a high level of sensitivity and is confided or collected in circumstances of vulnerability and trust for the primary purpose of benefiting the patient.
4. The hallmark of the medical profession since the time of Hippocrates has been the willingness and ability to hold information confided secret.
5. The patient-physician relationship is one of trust. A central feature of this trust is the belief of patients that information confided in or collected by physicians and other health care providers will be kept secret.
6. Patients believe that the information they disclose or that is gathered as a result of their seeking health care will be used to provide them with health care. Use beyond the provision of health care without knowledge or consent goes beyond what a patient's reasonable expectations were when information was confided or collected and therefore is a breach of the trust patients place in their physicians.
7. Except in very limited circumstances, consent is required for health information collection, use, disclosure or access for any purpose.
8. Information required to provide patients with the health care sought should be readily available to those who require it to provide an aspect of care as consistent with the wishes of the patient.
9. Uses of health information for purposes other than the provision of health care to the person seeking care should be subject to rules that:
 - protect and promote privacy and confidentiality;
 - generally require express consent;
 - can be justified according to specific criteria.
10. Patients should know the uses to which their health information may be put prior to disclosing it.
11. Patients may be reluctant to disclose information if they are concerned about the uses to which the information is put or the persons entitled to access it.

B. Public Opinion

To determine the public's views on issues concerning privacy and health information, CMA commissioned Angus Reid to conduct research in two forms, quantitative (survey) and qualitative (focus groups), and has found the

following:

1. Canadians believe that health information is the most sensitive type of information, and indeed more sensitive than their financial information.
2. Canadians believe that their health information will be kept confidential and consider this to be important.
3. Canadians believe it important to know and control how their health information is shared with others.
4. Canadians do not want their health information released to third parties (including governments and researchers) without their knowledge and consent.
5. Canadians have concerns about the release of delinked or anonymous information to third parties without their consent.
6. Some Canadians are reluctant to confide information to their physicians due to concerns about it subsequently being disclosed to others without their consent.
7. Patients believe that privacy rules should apply equally to the public and the private sector.

These findings are consistent with the published literature and other findings relating to the public's concerns about privacy and confidentiality. The CMA Health Information Privacy Code was developed in consideration of these views. Once developed, its principles were subsequently tested with the public in a series of cross-country focus groups and it was found that the Code appears to enjoy considerable public support.

C. The Advisory Council Report

The Advisory Council Report relates to the electronic health record. However, given the direction towards the greater use of technology and the underlying principles informing the Advisory Council, its recommendations are generalizable to all health information.

A key principle of the Advisory Council Report is that access by health care professionals should be based on a need-to-know basis under the strict control of the patient. The Council, like CMA, calls for scrutiny and justification of secondary uses of health information. The Council is opposed to the use of multipurpose identifiers on the grounds that it becomes too easy for government officials from one department to gain access to a person's health record or to combine a number of records to assemble a comprehensive profile. (Anecdotal evidence suggests that this concern may be justified and that there are insufficient safeguards preventing the flow of health information among government departments.) The Council recommends that all governments ensure that they have legislation to address privacy protection specifically aimed at protecting personal health information through explicit and transparent mechanisms. Included in these mechanisms are:

- The provision of a precise definition of free and informed consent, as well as a statement of principle that informed consent should be the basis for sharing personal health information;
- Any exemption to the requirement of informed consent should be clearly set out in law. More specifically, legislative guidance should be provided on how to balance the right of privacy with the public good for research purposes to implement a coherent and harmonized pan-Canadian system for independent, ethical review.
- There should be provisions regulating secondary uses of non-identifiable health information. These provisions should address privacy concerns surrounding the degree to which data might be linked back to an identifiable individual.
- Legislation should set clear limits on access to and use of health information by third parties outside the health care system. To prevent the serious invasions of privacy that can result from the unrestricted linking of personal health information with other kinds of information on the same individual, the legislation should contain provisions prohibiting the use for any other purpose of unique personal identifiers in health information systems.

D. The Approach in Bill C-6

Bill C-6 begins with the right premise: that “rules to govern information collection, use and disclosure” should recognize the “right of privacy”. However, it fails to recognize the special nature of health information and to tailor its provisions accordingly. In consequence, there is confusion and uncertainty about Bill C-6’s application to health care. Even more seriously, however, Bill C-6 fails to recognize that health information requires stronger or greater privacy protection than other types of information.

The Bill makes a cursory attempt at distinguishing among varying types of personal information and gives inadequate additional protection to information that is highly sensitive (such as health information), notwithstanding the provisions in Paragraph 4.3.4 of Schedule 1 concerning consent which do provide some latitude for more stringent requirements in the case of sensitive information. The Bill permits the collection, use and disclosure of information *without knowledge or consent* on grounds such as expediency, practicality, public good, research, offence investigation, historic importance and artistic purposes. In the context of health information, these grounds should be subject to intense scrutiny to determine their relevance and legitimacy. Some of these grounds would not withstand scrutiny if subjected to the tests established in the CMA’s Health Information Privacy Code.

E. Conclusion

CMA believes that health information is special and deserves a higher level of privacy protection than other types of information. The Advisory Council Report also recognizes that distinct rules, more protective of privacy, are required for health information. The Council’s Report places strong emphasis on the protection of

privacy, recognizes that, as a general rule, the flow of health information should be on a need-to-know basis and under the control of the patient through the exercise of free and informed consent, and requires limits on the secondary use of health information.

The inadequacy of Bill C-6 for health care is not surprising because clearly it was not drafted with health information in mind. Rather, it is written from the perspective of encouraging commerce. It appears to have access to information as its dominant value. However, the world of health care is very different from that of commerce and distinct rules that are more protective of privacy.

The CMA Health Information Privacy Code begins from the same starting point as Bill C-6, the Canadian Standards Association (CSA) Code which the Bill includes as Schedule 1. However, unlike Bill C-6, the CMA Code tailors the CSA Code to the specific circumstances of health information. The CMA Health Information Privacy Code, therefore, is able to address issues specific to health information that Bill C-6 either fails to address or, even worse, creates. It offers a template for the protection that should be specifically accorded to the right of privacy in health information, a template that appears to have considerable public support and is designed to uphold patient confidence in their physicians and the health care system.

Amending Bill C-6 to incorporate the principles in the CMA Code would ensure adequate privacy protection. CMA recommends:

That Bill C-6 be amended to incorporate specific provisions relating to health information and that the provisions of the CMA Health Information Privacy Code provide the basis of such provisions.

CMA developed the Health Information Privacy Code in recognition of trends and developments that pose new threats to patient privacy and the trust of the therapeutic relationship. In recent years the secondary use of information for purposes other than the purposes for which it was collected has been increasing without adequate oversight or public knowledge. This 'function creep' undermines the trust of patient-physician relationship. Collection and use beyond the therapeutic context and for purposes unrelated to the provision of direct care should be subjected to rigorous scrutiny before they are permitted to occur. To the extent that they are permitted to occur without patient consent they should be explicitly authorized in legislation to ensure transparency and adequate oversight.

CMA's Health Information Privacy Code provides a test to which legislation addressing health information should be subjected. This test (found in section 3.6 of the CMA Code) states:

Any proposed or existing legislation or regulation made under legislative authority that permits or requires health information collection, use, disclosure or access shall be subjected to the following legislative test:

- (a) There must be demonstration that:

- (i) a patient privacy impact assessment has been conducted, the analysis has been made public and has been duly considered prior to the introduction of legislation [section 3.5 of the Code provides guidance with respect to the patient privacy impact assessment];
 - (ii) collection, use, disclosure and access will be limited to the greatest degree possible to ensure that
 - the collection of health information by persons external to the therapeutic context will neither trade on nor compromise the trust of the patient-physician relationship;
 - patients are not likely to be inhibited from confiding information for primary purposes;
 - the ability of physicians to discharge their fiduciary duties to patients will not be compromised; and,
 - patient vulnerability will not be exploited;
 - (iii) collection, use, disclosure and access will be restricted to what is necessary for the identified purpose(s) and will not impede the confiding or collection of information for primary purposes;
 - (iv) provisions exist for ensuring that patients are provided with knowledge about the purpose(s) and that, subject to 3.6(b), patient consent is clearly voluntary;
 - (v) the means used are proportionate and the collection will be limited to purposes consented to or made known to the patient;
 - (vi) the patient's privacy will be intruded upon to the most limited degree possible in light of the purpose(s) consented to or made known to the patient;
 - (vii) linkage of the health information will be limited; and
 - (viii) unless clear and compelling reasons exist:
 - all reasonable steps will be taken to make health information anonymous; and
 - if it has been demonstrated that making health information anonymous would render it inadequate for legitimate uses, the information will be collected and stored in a deidentified-relinkable format.
- (b) When nonconsensual collection, use, disclosure or access is permitted or required by legislation or regulation that meets the requirements of the Code, the following conditions must also be met:
- (i) the right of privacy has to be violated because the purpose(s) could not be met adequately if patient consent is required; and
 - (ii) the importance of the purpose(s) must be demonstrated to justify the infringement of the patient's right of privacy in a free and democratic society.
- (c) Any legislative provision or regulation that permits or requires health information collection, use, disclosure or access non-

consensually shall not, without compelling reasons, be applied retroactively to existing health information.

In its current form, Bill C-6 would not pass the scrutiny of the test. Consequently, CMA recommends:

That the proposed rules for health legislation be subject to the legislative test found in CMA's Health Information Privacy Code and formulated in light of this process.

IV. Specific Comments on Bill C-6 From the Perspective of CMA's Health Information Privacy Code

This section highlights some key distinctions between the approach taken by Bill C-6 and CMA's Health Information Privacy Code. It uses examples to illustrate divergent approaches taken for the purpose of demonstrating that Bill C-6 is inadequate in the protection it accords health information and to show how the CMA Health Information Privacy Code would address the issues adequately.

A. General

Bill C-6 and CMA's Health Information Privacy Code are based on the Canadian Standards Association's Model Code for the Protection of Personal Information (CSA Code). Bill C-6 and the CMA Code also augment the CSA Code's provisions where considered necessary. The need to extend the provisions of the CSA Code demonstrates that the CSA Code, being general in nature, provides inadequate protection to information in many instances. The CSA recognized this at the time it developed its Code and specifically issued additional, specific guidance for health information in the form of an appendix to the Workbook for applying the Code. The Workbook begins:

Information regarding one's health and health records may be among the most sensitive of all personal data. Individuals are concerned that inappropriate disclosure of such information could unduly affect their employment status or their lives in general. . . Some health information is obtained directly from health care providers who have been given a patient's private information with the expectation that this information will remain as a private communication. Health care providers . . . in turn, feel that such concerns could influence individuals to withhold vital information or avoid treatment to ensure their private information remains as such. Implementation of privacy procedures that adhere to the principles in the CSA Code and rigid applications of such procedures are essential steps for organizations that require access to health information, to maintain an individual's trust that sensitive personal information remains confidential. In designing and implementing such procedures, organizations should recognize the sensitive nature of such information and also the fact that the primary reason that health care providers

maintain records is to ensure that safe and efficacious care is provided.

The Workbook goes on to list 7 interpretative points to augment the CSA Code, providing additional privacy protection as it applies to health information, including the following:

requirements for the individual's *knowledge* and consent be rigidly followed. Consent to acquire and disclose health information should be undertaken with the individual's full knowledge of the scope of information to be requested.

Bill C-6 does not include these additional interpretive points. It does not give due recognition that health information, because of its high sensitivity, deserves even stronger protection than is provided in the CSA Code as appended in Schedule 1 of the Bill (which even the Committee that drafted the CSA Code recognized).

Although Bill C-6 and the CMA Code are based on the CSA Code, each takes a different approach to the ultimate protection accorded information and to the right of privacy. This divergence demonstrates that there are many ways to resolve issues left unresolved by the CSA Code. In other words, it is not a foregone conclusion that basing provisions on the CSA Code will result in appropriate or adequate protection of information. Rather, resolution of issues requires thought and deliberation and will depend in some measure on the primacy given to certain values. Bill C-6 appears to have given access primacy in the pursuit of commerce, whereas CMA gives privacy protection primacy in the pursuit of the provision of health care in accordance with physicians' fiduciary obligations to patients and the integrity of the patient-physician relationship.

CMA did not develop its approach in a vacuum. It reviewed, and was inspired by, the report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, entitled *Privacy: Where Do We Draw the Line?* This report articulates and makes explicit many of the issues that should be informing the current debate on Bill C-6. In addition, the Report of the Advisory Council takes a very different approach than Bill C-6. The Report recognizes the need to pay more than lip service to protecting privacy and confidentiality and recommends specific measures aimed at doing this.

B. Primacy of the Therapeutic Purpose

The root of most of the problems in applying Bill C-6 to health care is its failure to distinguish among purposes for the collection, use and disclosure of health information. In particular, the Bill fails to distinguish between the primary purpose, which is to deliver care to and for the benefit of an individual patient, and secondary purposes, which are not for the direct benefit of the patient and indeed may even involve using the patient's information to his or her detriment. Under Bill C-6, the same rules apply

equally to both the primary and to secondary purposes. In other sectors this failure to distinguish different purposes and to fashion rules in light of salient differences may not pose problems. In the health care sector, however, the consequences could be quite serious.

As applied to secondary purposes, the provisions in Bill C-6 fail to limit access appropriately. Access to information may occur in ways that are inappropriate and violate the privacy of patients. As applied to the primary purpose -- the use of a person's information to provide that person with care -- the rules in the Bill, if rigidly construed, may inhibit access that would otherwise be appropriate and consistent with the patient's right of privacy. For example, the consent provisions in the Bill could create impediments to information flow where various members of a 'health care team' require information about the patient in order to be effective for the patient's benefit; the provisions in the Bill that seek to limit the extent of information collection could inhibit physicians from being as extensive as they sometimes are and should be in collecting information from patients for the purpose of providing care; the provisions in the Bill requiring that the patient's request to review his or her record be in writing could in fact be a barrier to patient access which might otherwise be facilitated informally and consistently with the patient's wishes by a simple verbal request.

Such consequences no doubt would be unintended by the drafters of the Bill; the drafters might even argue that for someone to interpret the provisions mentioned above as potentially leading to these consequences would be to misinterpret them. Regardless, the fact is that the Bill, on these matters and others, is somewhat strained when its provisions are applied to health care.

The CMA Health Information Privacy Code, however, is not. It begins from the same starting point as Bill C-6, which is the CSA Code. However, the CMA, recognizing (as the drafters of the CSA Code apparently also did) that the CSA Code would need to be tailored to deal adequately with health information, did so in drafting its Health Information Privacy Code. This document was written from the ground up not just with privacy first and foremost as a value but also with specific reference to the health sector. And it is based on the fundamental premise that not all purposes for the use of health care are equal and that the therapeutic purpose must be given primacy.

Thus the CMA Health Information Privacy Code avoids the kind of problems identified above that might arise as Bill C-6 is applied to health information. For example, it specifies that the collection of health information for the primary purpose of providing care "may be as extensive as necessary to fulfil these purposes and reflect the high level of trustworthiness and accountability of health professionals in the therapeutic context" (3.2) but that for any secondary purposes it should be "as minimal as necessary in recognition of the need to protect the patient's right of privacy in the therapeutic context" (3.3.).

As concerns consent, which CMA recognizes to be core to the protection of privacy, the CMA Code articulates rules for consent in recognition of the

importance of timely information flow in the team context and as appropriate to meet the purpose for which the patient has confided the information in the first place, which is to receive care. It stipulates that consent for the primary purpose may therefore be implied, albeit with certain qualifications. Moreover, where consent is required, the provisions of the Code allow that “the conveyance of generic information is a reasonable means of providing knowledge” in most circumstances, which means that this requirement is unlikely to create unreasonable burdens that would diminish rather than strengthen the therapeutic relationship.

Finally, the CMA Code limits itself to issues of principle concerning patient access to their records; Bill C-6, by specifying that requests must be in writing, could in fact be creating a barrier to patient access or an undue burden upon the patient-physician relationship as there may be instances when an informal request would be quite appropriate.

C. Knowledge of Purpose Prior to Collection

Bill C-6

Bill C-6 is ambiguous in its provisions relating to whether or not a person should know the purposes for which information will be used prior to disclosure. This is due in part to the use of the term “knowledge and consent” as one concept rather than distinguishing the knowledge requirement from the consent requirement. What a person should know in relation to the purposes for which information might be used or disclosed, prior to its being given, is distinct conceptually from whether the person must consent before information can be used or disclosed for a particular purpose.

Schedule 1 of the Bill contains a number of principles. For the purposes of this Brief the schedule will be referred to in terms of the principles (and their subparagraphs). Principle 2 addresses the identification of purposes for which information will be used or disclosed. Provided a purpose is identified it becomes a legitimate purpose (this Brief recognizes that the addition of the “reasonable person” clause in 5(3) takes precedence and provides some grounds for distinguishing legitimate and illegitimate purposes). Subparagraph 3 states that the identified purposes *should* be specified at or before the time of collection. Section 5(2) of the Bill states that the use of ‘should’ in schedule 1 indicates a recommendation and does not impose an obligation. Therefore, according to subparagraph 3, it is recommended but is not obligatory that disclosure occur.

On the other hand, principle 3 addresses consent and appears to impose an obligation by stating that the knowledge and consent of the individual *are required* for the collection, use, or disclosure of personal information, except where inappropriate. Similarly, subparagraph 2 appears to create something of an obligation by stating, “organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used.”

Section 7(1)(a) permits the collection of information without knowledge and consent when collection is clearly in the interests of the individual and consent cannot be obtained. The intent of this section could be made clearer, particularly in terms of who determines the “interests of the individual.” Otherwise this exception could give undesirable licence to collect without knowledge or consent.

The provision in section 7(1)(b) is more problematic. This section appears to favour withholding knowledge from an individual if such knowledge would compromise accuracy, defeat the purpose for collection or prejudice the use. In some instances it may well be that, if an individual is provided with knowledge of the purposes for which information is collected and the uses to which it will be put, he or she may choose to withhold information rather than disclose it, and in doing so would clearly compromise accuracy, defeat the purpose for collection or prejudice the use to which the information will be put. This is contrary to principle 4.4.2, which recognizes that information should not be collected by misleading or deceiving individuals. The intent of this section should be far clearer and circumscribed in such a way as to make it clear that it is not permissible to withhold knowledge or not seek consent simply on the basis that if a person had knowledge they would not wish to disclose information.

Section 7(1)(c) allows collection without knowledge or consent for journalistic, artistic or literary purposes. This provision is totally inappropriate in the case of health information.

CMA Health Information Privacy Code

The CMA Health Information Privacy Code is considerably more restrictive than Bill C-6. It recognizes that, in the therapeutic context, health information is confided or collected under the patient’s presumption that it is necessary to meet his or her therapeutic needs. The potential that health information may be subsequently collected, used, disclosed or accessed for other purposes without patient consent should be made known to patients before information is confided or collected for the primary therapeutic purpose. Moreover, it is not acceptable to withhold knowledge from patients deliberately out of concern that knowledge could inhibit them from confiding important information fully and truthfully.

The CMA Health Information Privacy Code limits the nonconsensual collection of health information to circumstances where it is either permitted or required by legislation or ordered or decided by a court of law. In addition, the CMA Code gives explicit direction to legislators with respect to the conditions under which legislation should permit or require health information collection (see section 3.6 of CMA Code). In the case of nonconsensual collection, the following conditions are stipulated:

1. The right of privacy has to be violated because the purposes could not be met adequately if patient consent is required; and

2. The importance of the purposes must be demonstrated to justify the infringement of the patient's right of privacy in a free and democratic society.

D. Use Without Knowledge Or Consent

Bill C-6

Once information has been collected and despite the limits, inadequate though they be, placed on collection without knowledge or consent, it can be put to even greater use than for the purposes for which it has been collected (with or without knowledge or consent). Section 7(2) opens up dramatically the uses to which collected information may be put without either knowledge or consent. At a minimum, and with little additional administrative effort, the enumerated grounds of section 7(2) (and 7(3)) should be made known to an individual prior to their disclosure of information, which would be in keeping with the principle of openness and explicitness.

Section 7(2)(a) allows use in connection with the investigation of an offence. In the medical context this could be problematic, particularly if it is interpreted to impose an obligation. Generally, there is no obligation to assist in the investigation of an offence, and indeed the fiduciary duty between patient and physician and the duty of confidentiality owed to the patient by the physician would suggest that physicians not offer information, despite its usefulness.

Section 7(2)(b) recognizes emergency situations. However, as worded, section 7(2)(b) would allow access to anyone's information if it is for the purpose of acting in an emergency threatening the life, health or security of *an* individual. The implications of this section should be carefully thought through. It is not desirable to give such a broad licence to access anyone's information on the basis of an emergency. There should be some limiting principle that takes into account the prevailing view that people generally are not *required* to go to the assistance of others (emergency or otherwise) and that information about oneself is considered worthy of protection against use or disclosure, despite its potential benefit to others (for example, genetic information or HIV or Hepatitis C status).

Section 7(2)(c) is very problematic as it permits the use of "identifiable" information for a host of purposes, including statistical and research, when it is impractical to seek consent. Even though the Commissioner must be informed of the use before the information is used the Commissioner has no power to approve or reject the use. If the use is legitimate under the Bill there would be no grounds open to the Commissioner to cause an audit to occur. This section gives significant scope for the secondary use of information that has been collected without knowledge or consent; in the case of health information it is very problematic.

CMA Health Information Privacy Code

The CMA Code makes a clear distinction between the primary purpose for the collection and use of health information and secondary purposes for its use. The key distinction between these two categories is that primary purposes relates to the provision of the health care benefit sought whereas secondary purposes are ends or aims that are not directly related to the provision of care. The CMA Code divides secondary purposes into two categories:

1. Secondary legislated purposes are those purposes that have been subjected to the legislative test specified in the Code and have subsequently been written into law;
2. Secondary non-legislated purposes are any other purposes, such as education or research not governed by legislation, that meet the provisions of the CMA Code and the secondary non-legislative test provided by the Code.

The tests that the CMA Code requires of both relate to:

1. Impact on privacy.
2. Impact on the patient-physician relationship, especially confidentiality and trust.
3. Impact on the willingness of patients to disclose information.
4. Impact on patients' ability to receive care.
5. Evidence of broad public support for the measure.
6. The use will not exploit or compromise the trust of the patient-physician relationship.
7. Patient vulnerability will not be exploited.
8. Under most circumstances patients will be fully informed of the purpose and patient consent will be clearly voluntary.
9. Patient privacy will be intruded upon to the most limited degree possible.
10. Linkage of health information will be restricted and consented to by patients.

In other words, the CMA Code does not permit any and all secondary purposes for the use of health information. Rather, it requires justification for the secondary use and assurance that the secondary use will neither impede nor undermine the patient-physician relationship and the provision of health care to the patient. This test is much more privacy protective than the "reasonable person" test the Bill contains in Section 5(3). Moreover, the CMA Code only permits use without consent if it is permitted or required by legislation or when ordered or decided by a court of law.

The Advisory Council Report

Like the CMA, the Advisory Council Report makes distinctions among various types of uses. The Report calls for legislation to clearly prohibit all secondary commercial use of personal health information (in which respect the Advisory Council takes an even stronger position than the CMA). In

addition, the Report recommends that there be provisions regulating secondary uses of non-identifiable health information and that such provisions should address privacy concerns surrounding the degree to which such data might be linked back to an identifiable individual. In this context, the Report recommends that legislation set clear limits on access to and use of health information by third parties outside the health care system.

In addition the Report reviews the uses of health information for statistical and research purposes. In connection with research, the Report calls for a number of safeguards and restrictions:

1. Where the data sets used have a higher level of potential identifiability, “the general rule should be informed consent and stringent assurances about privacy protection and security arrangements are necessary before a researcher can have access to personally identifiable information.”
2. The Report recognizes that in some instances it may be impractical to obtain consent from patients. Whether in anonymous or identifiable form, the Report requires that notice be given about the use of the information. In the case of the use of identifiable information, the Report states that the research should be subject to independent ethics review with the onus on the person seeking to use the information without consent to demonstrate that:
 - (a) a tangible public good of significant benefit will result;
 - (b) consent is impossible to secure at a reasonable cost;
 - (c) less identifiable data will not serve the same purpose; and
 - (d) no harm can occur to any person directly or indirectly as a result of this use of his or her personal information.

E. Disclosure Without Knowledge Or Consent

Bill C-6

The comments found under C. and D. above apply equally here. Section 7(3) adds further instances when collected information can be disclosed to others without knowledge or consent.

CMA Health Information Privacy Code

In the case of secondary use of health information, the CMA Code takes a far more restrictive approach. As concerns use, disclosure or access, it states:

The potential that health information, in whole or in part, may be subsequently collected, used, disclosed or accessed for other purposes without their consent, and what those purposes might be, must be made known to the patient by reasonable means before it is confided or collected for primary purposes.

Moreover, the CMA Code recognizes that information disclosed by one

organization is *collected* by another. The Code defines collection to mean:

the act of accessing, receiving, compiling, gathering, acquiring or obtaining health information from any source, including third parties, and by any means. It includes information collected from the patient, as well as secondary collection of this information in whole or in part by another provider or user.

The collecting organization should be bound by the provisions of the CMA Code, which generally requires consent for use for any purpose and always requires knowledge of the potential purposes that information will or must be put to prior to the information being disclosed. CMA's Code states:

Health information custodians must ensure that third parties privy to health information have adopted this Code or are bound by equivalent provisions.

Finally, the CMA Code explicitly recognizes that information can be retrieved from a variety of sources to formulate records. Any and all such practices and the composite form developed are given the same degree of protection as that accorded information collected directly from the patient.

F. Consent

Bill C-6

In those cases where consent for collection, use or disclosure are required, the provisions in Bill C-6 are inadequate as applied to health care. Schedule 1 distinguishes between express and implied consent. Express consent is not adequately defined and it appears that this is not equivalent to what in health care is called 'informed consent'. For example, Principle 4.3.2. says that "organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used". In the health care context, the notion of 'reasonableness' with respect to the doctrine of informed consent applies not to the effort to advise or inform (that much is assumed or given) but rather to determinations regarding what information should be provided to the patient. In addition, the application of some of the means described in Principle 4.3.7 by which individuals can give consent, and in particular the 'negative option' checkoff box in (b), may be quite problematic in the health care context.

The broad scope allowed to implied consent in the Bill is also worrisome as applied to the health care setting. Principle 4.3.6 says "implied consent would generally be appropriate when the information is less sensitive". However, with implied consent the issue is not the sensitivity of the information but rather the wishes of the patient. It is appropriate to infer consent even when the information is very sensitive provided one has reason to believe this is grounded in the patients wishes; conversely, it is not appropriate to infer consent, even in the case of information deemed not to be sensitive, if there is reason to believe the patient would object if asked explicitly.

CMA Health Information Privacy Code

The CMA Code furnishes clear definitions for consent:

“Consent” means a patient’s informed and voluntary agreement to confide or permit access to or the collection, use or disclosure of his or her health information for specific purposes.

For purposes other than the provision of direct care, which is the purpose for which the patient presents in the first place, the consent must always be explicit or express since there is no logical connection between secondary purposes and the desire to achieve care. Therefore inferences cannot be made with any confidence. The Code defines express consent as follows:

“Express consent” is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the provider seeking consent.

The CMA Code defines implied consent to disallow the loose use of the term, which is increasing today, to justify access for purposes (secondary purposes in particular) that the patient may not wish to occur:

Implied consent arises where agreement may reasonably be inferred from the action or inaction of the individual and there is good reason to believe that the patient has knowledge relevant to this agreement and would give express consent were it sought.

The CMA Code also lays out clear rules for the use of the concept of consent and makes clear that consent can be inferred for primary purposes (i.e., the provision of health care to the patient) but not for secondary ones, which require express consent. The Code grounds the notion of implied consent not in the desire to subvert express consent and thereby gain access to information that might otherwise be denied but rather in the wishes of the patient and the importance of providing health care for therapeutic purposes as consistent with those wishes.

Advisory Council Report

In addition to being more stringent than Bill C-6 about exemptions to consent, the Advisory Council Report also gives greater importance to defining the term clearly and strictly. It says that any legislation concerning health information should:

contain a precise definition of free and informed consent, as well as a statement of principle that informed consent should be the basis for sharing personal health information.

Although not as precise and emphatic on the subject of consent as is the CMA Health Information Privacy Code, the Report is certainly more so than is Bill C-6.

G. Information Flow Within Organizations

Bill C-6

Bill C-54 defined use to include “the transfer of personal information within an organization.” Bill C-6 no longer defines use, which leaves it uncertain whether the definition of use quoted above from Bill C-54 would be a reasonable interpretation of Bill C-6. If so, this would create a problem. Interpreting use in this way could have the effect of inappropriately restricting the free flow of information within an organization. In the health care context this is not a reasonable or desirable outcome and would hinder, rather than promote, the patient’s right of privacy.

CMA Code

The CMA Code recognizes that the free flow of health information is desirable to the extent that it furthers the provision of the health care benefit sought and that it occurs with patient consent. The Code defines the primary purpose to mean:

- (i) Primary therapeutic purpose is the initial reason for a patient seeking or receiving care in the therapeutic context, and pertains to the delivery of health care to a particular patient with respect to the presenting health need or problem. It encompasses consultation with and referral to other providers on a need-to-know basis.
- (ii) Primary longitudinal purpose concerns developing composite health information about a particular patient, such as a detailed medical history, beyond direct application to the presenting health need or problem, in order to enhance ongoing care to that person.

The Code goes on to state that:

Health information collection, use, disclosure or access for the primary therapeutic and longitudinal purposes may be as extensive as necessary to fulfil these purposes and reflect the high level of trustworthiness and accountability of health professionals in the therapeutic context.

And further states that:

Security safeguards shall impede as little as possible health information collection, use, access and disclosure for primary purposes.

Finally, in addressing consent the Code states:

Consent to health information collection, use, disclosure and access for the primary therapeutic purpose may be inferred. Consent to subsequent collection, use, disclosure and access on a need-to-know basis by or to other physicians or health providers for this purpose, and for this purpose alone, may be inferred, as long as there is no evidence that the patient would not give express consent to share the information.

The principles in the CMA Code that give effect to the patient’s right to

control what happens to his or her information are not incompatible with the free flow of information among members of a health team for the purpose of providing care to the patient. Indeed, they facilitate and enable this flow to the extent this is in keeping with the patient's wishes.

H. Information Protected

Bill C-6

The Bill covers "personal information" which is defined to mean "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." This definition raises a host of questions:

1. Does the Bill cover information that has been delinked to an identifiable individual but that could be relinked to identify them?
2. Does the Bill only exclude anonymous information - that is, information that could never be relinked to an identifiable individual? And if so, is there an unjustified assumption that information can, in all cases, be rendered truly anonymous?
3. In the case of delinked and anonymous information, who decides that information about an identifiable individual can be rendered delinked or anonymous? The holder of the information or the person to whom the information pertains?
4. Is it accurate or reasonable to assume that people have no interest in information emanating from them once it has been rendered delinked or anonymous?
5. Given that anonymous information is generated from personal information, is the act or process rendering personal information into anonymous form considered a use under the terms of the Bill, and if so does this use require consent?

In considering these questions, it is important to keep in mind that the concept of "anonymity" means different things to different people. Moreover, there are no generally used or accepted standards that address what is required to render identifiable information truly anonymous. As a consequence, different people use different standards (of varying degrees of rigour), if they use a standard at all. It is also important to note that, in virtue of sophisticated techniques for identifying individuals from supposedly anonymous information, there is debate about the extent to which true anonymity can ever be achieved or guaranteed.

CMA Health Information Privacy Code

In light of issues concerning the definition of 'personal information' and in

the interest of ensuring a thorough scrutiny of information practices, the CMA Code provides a broad definition of health information:

Health information means any information about a patient that is confided or collected in the therapeutic context, including information created or generated from this information and information that is not directly or indirectly linked to the provision of health care. It includes all information formats.

The CMA Code covers identifiable information, delinked information, anonymous information and any composite form that is produced when health information is linked to other information about the patient. CMA's research indicates that patients have an interest in their information even when it is in delinked and in anonymous formats. This view has recently received support from a decision of the High Court of Justice in England that is particularly relevant in the context of the commercial use of health information (Source Informatics Ltd. v. Department of Health). The issue arose because a prescription database company sought judicial review of a Department of Health policy document that advised National Health Service GPs and pharmacists not to sell "anonymous" prescribing or dispensing information. The document contained the following analysis:

Anonymisation (with or without aggregation) does not, in our view, remove the duty of confidence towards the patients who are the subject of the data. Apart from the risk of identification of a patient despite anonymisation, the patient would not have entrusted the information to the GP or the pharmacist for it to be provided to the data company. The patient would not be aware of or have consented to the information being given to the data company, but would have given it to be used in connection with his care and treatment and wider NHS purposes. Anonymisation of the data (with or without aggregation) would not obviate a breach of confidence. . . .The duty of confidence may in some circumstances be outweighed by the public interest in disclosure. However we have severe reservations that disclosure by GPs or NHS pharmacists of dispensing information to X or other data companies would be argued to be in the public interest. Indeed it might well be contrary to the public interest if the data company is further selling the information on doctors prescribing habits to the pharmaceutical industry.

High Court Justice Latham upheld the policy document, arguing that the information in question, though anonymous, was nonetheless confidential. He also argued that consent to its release was necessary and could not be implied, and that the breach of confidentiality involved in selling this information could not be justified as being in the public interest:

In my view, it is impossible to escape the logic . . . that the proposal involves the unauthorised use by the pharmacist of confidential information. . . . In my judgement what is proposed will result in a clear breach of confidence unless the patient gives consent, which is not part of the proposal at present. Nor is it suggested that the patient can be said to have given implied consent. . . . I recognize that, for some, the sensitivity, as they see would see it, of the information may be such that they would feel that any use of the information without their consent, would be unconscionable. In other words it would be a breach of trust which they were reposing in the pharmacist. . . . I have come to the conclusion that . . . this [is] a type of situation . . . in which there is a public interest in ensuring that confidences are kept. It is important that those who require medical assistance should not be inhibited in any way from seeking or obtaining. As I have indicated, I believe that there may be some patients who will feel very strongly that the pharmacist should not give any information obtained from the prescription without their consent.

In view of the fact that there is a growing industry in so-called anonymous health information, it is important to ensure that this information is protected as consistent with the duties of health care providers and the expectation patients have that their providers will keep their information confidential.

Advisory Council Report

The Advisory Council Report addresses this issue in a number of ways. In making recommendations concerning the definition of health information, the Report calls for legislation that embodies:

a clear definition of health information, broad enough to incorporate health information collected in public and private systems and to ensure that equal obligations and penalties apply to both public and private sectors.

The Report recognizes a spectrum of data formats: completely anonymous, linked to pseudo-identities, code linked and re-identifiable, completely identifiable. In terms of sensitivity, the Report notes that information that can be re-identified is somewhat more sensitive than completely anonymous data or anonymous data linked to pseudo-identities and that completely identifiable health information is the most sensitive type of health information. The Report also notes that there can be some degree of risk of re-identification of what was believed to be anonymous data through such processes as data matching and the results of analysis using small cells. In this light, the Report recommends that legislation should recognize:

A definition of personal health information, which takes into account the spectrum of potential identifiability in the case of health information.

Furthermore, in the case of secondary uses of health information, the Report

notes that provisions regulating secondary uses of non-identifiable health information must form part of any comprehensive legislation. Such provisions should address privacy concerns surrounding the degree to which data might be linked back to an identifiable individual.

The Report raises further issues relating to the use of delinked and anonymous data. The Report notes that there may be group interests and concerns regarding data collected and states:

Privacy can also be a concern for groups such as Aboriginal and immigrant communities. These communities worry that research on their members could be released to the media without notice and used in a negative way. This emerging issue is growing in importance and, in the Council's view, should be a serious consideration in the context of ethical reviews of proposed research projects.

It is important to note that, in these instances, it is not the fact that data is linked to an identifiable individual that is of concern. Rather, it is the ability to accumulate, process and dissect information that has ramifications for an individual because they are part of a group segregated and identified by the research.

Finally, the Report considers the use of person-oriented data (data linked to individuals in a form where personal identifiers have been replaced by a code) for statistical purposes and notes that this too raises concerns about privacy. The Report notes that:

"These concerns have traditionally been seen as a trade-off against data access for research and analysis in the public interest."

The Report restates this to provide a more positive view of privacy and states:

the best way for analysts to maintain the public's consent to use sensitive (but anonymous) health data is to show the public that privacy, confidentiality and security are being taken seriously.

In view of the issues concerning the definition of personal information and in the interest of ensuring maximum scrutiny of practices concerning health information and maximum protection of the right of privacy with respect to health information, CMA recommends:

That there be a clear definition of the information being accorded a right of privacy and that this definition, at least in the case of health information, include identifiable information, delinked information, anonymous information and any composite information produced when health information is linked to any information about a person from any other source.

I. Individual Access

Bill C-6

Bill C-6 restricts the right of individual access to personal information. The grounds for denying access to information are inappropriate in the health care context.

CMA Code

The CMA Code follows the prevailing case law as it relates to medical records. Primarily this gives patients a right of access to their record in all but very limited circumstances. These circumstances are when there is a significant likelihood of a substantial adverse effect on the physical, mental or emotional health of the patient or substantial harm to a third party. The onus lies on the provider to justify denial of access on these grounds.

J. Accuracy and Amendment

Bill C-6

Bill C-6 requires that information be as accurate, complete and up-to-date as possible and that it shall not be routinely updated unless this is necessary to fulfil the purpose for its collection. In so far as amendment is concerned, Bill C-6 permits amendment to the record in specified circumstances.

CMA Code

The CMA Code takes a different approach in light of the nature and purpose of health information. The Code recognizes that the

recording of statements of fact, clinical judgements and determinations or assessments should reflect as nearly as possible what has been confided by the patient and what has been ascertained, hypothesized or determined to be true using professional judgement.

In terms of amending the record in light of a patient's request, the CMA Code seeks to preserve the original record but also provide for noting the patient's concerns. To accommodate both requirements the CMA Code states:

Patients who have reviewed their information and believe it to be inaccurately recorded or false have the right to suggest amendments and to have their amendments appended to the health information.

K. Sensitivity

Bill C-6

Schedule 1 recognizes that medical records have a high level of sensitivity attached. For this reason this information may warrant special attention

concerning consent, reasonable expectations, individual access and the degree of security that is appropriate.

CMA Code

The CMA Code recognizes that, even as all health information is sensitive (when considered against other forms of information about individuals), there are also variations in the level of sensitivity in various aspects of the health record. The CMA Code defines the “sensitivity of health information” to refer to:

the patient’s interest in keeping the information secret. It varies according to the nature of the information, its form, and the potential negative repercussions of its collection, use or disclosure on the patient’s interests.

Under the Code’s consent provisions it is stated that:

Although all health information is sensitive and should be treated as such, the more sensitive the health information is likely to be, given what is known about the circumstances or preferences of the patient, the more important it is to ensure that consent is voluntary and informed.

With respect to security the Code states:

The development of security safeguards with respect to levels of access for various users shall recognize the differences in the sensitivity of health information and permit access accordingly.

Moreover, the Code recognizes that health information is special and therefore requires distinct rules that afford stronger privacy protection not just due to its sensitivity but also to the circumstances of vulnerability and trust under which it is initially confided or collected. These special circumstances, which include much more than sensitivity, are outlined in Principle 2 of the Code. Bill C-6, by contrast, fails to consider these other features that make health information a special case. In consequence its provisions are not adequately tailored to the special nature of health information and do not accord it the strong privacy protection it warrants.

V. Conclusions

The increased capacity to collect, store, transfer, merge and access information, coupled with trends that support increased use of and access to information, have the potential to erode our traditional understanding and protection of privacy and confidentiality. The issues are complex and the choices we must make are difficult. Nevertheless, these issues should be squarely on the table and the choices that we make must be clear, transparent and defensible.

Of paramount importance is that the public is not misled into believing that their information is being protected or kept confidential when in fact it is not. Therefore,

even to refer to Bill C-6 as the “Personal Information Protection and Electronic Documents Act” should be the subject of debate. Is the Bill truly about information protection or is it actually about permitting access to information?

The approach to rules for information in Bill C-6 is directed toward commerce and appears to have access, and not privacy, as its dominant value, notwithstanding the Bill’s reference to a “right of privacy”. In CMA’s view, the Bill’s approach is inadequate when applied to health information. Based on the evidence, it seems highly likely that the public would also find Bill C-6 inadequate.

Bill C-6 was not developed with health information in mind. In consequence there is confusion and uncertainty about its application to the health care context. Even more seriously, however, Bill C-6 fails to recognize that privacy with respect to health information requires stronger or greater protection than other types of information.

CMA presents a different approach, an approach that recognizes the special nature of health information; an approach that puts patients first and values privacy and the preservation of the trust and integrity of the patient-physician relationship. This approach appears to be well-grounded in the values that Canadians hold about privacy and would likely enjoy broad public support. In addition, the CMA approach draws support from the Federal Advisory Council Report, which like CMA recognizes the importance of preserving patient privacy and the confidentiality of the health record in an era of increased use of technology. Implicitly, the Report recognizes that the benefits of such technology cannot be realized if public support, based on respect for privacy, cannot be secured.

The CMA’s Health Information Privacy Code does what Bill C-6 fails to do. Amending Bill C-6 to incorporate the principles in the CMA Code would ensure adequate privacy protection. In light of the clear deficits in Bill C-6 and the inadequate protection of patient privacy and health information confidentiality, CMA urges this Committee to accept its recommendations and the amendment that incorporates them. Nothing less would give Canadians the high level of privacy protection they desire and deserve when it comes to their health information.

VI. Summary of Recommendations

That Bill C-6 be amended to incorporate specific provisions relating to health information and that the provisions of the CMA Health Information Privacy Code provide the basis of such provisions; and

That any proposed rules for health legislation be subject to the legislative test found in CMA’s Health Information Privacy Code and formulated in light of this process; and

That there be a clear definition of the information being accorded a right of privacy and that this definition, at least in the case of health information, include identifiable information, delinked information, anonymous information and any composite information produced when health information is linked to any other information about a person from any other source; and

That, at least in connection with health information, the provisions of the Bill apply equally to the public and the private sectors.

CMA has drafted an amendment to Bill C-6 (Appendix B) which, if accepted, would achieve all of these recommendations and adequately give Canadians the kind of privacy protection with respect to their health information that they deserve and desire.